NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

October 6, 2008 | 1 p.m. – 5 p.m.
October 7, 2008 | 8 a.m. – 5 p.m.
October 8, 2008 | 8 a.m. – 12 p.m.
National Institute of Standards and Technology, Gaithersburg, MD

MEETING SUMMARY CONTENTS

Meeting Facilitation and Draft Report By: Robert Jones, Stuart Langton & Hal Beardall
FCRC Consensus Solutions- Florida Conflict Resolution Consortium**, Florida State University**

Thanks to Team members Sharon Edwards, Kevin Perry and Tom Hofstetter for sharing their meeting notes.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and reviewed with the Standard Development Team (SDT) and participants the proposed meeting agenda. Team Members introduced themselves highlighting a broad spectrum of expertise and industry and governmental perspectives and a shared expectation that they would keep the needs of the industry in mind, but do the right thing. Several noted the importance of engaging and involving Canada in the standards development process. Others pointed to the fact the industry must successfully respond to the cyber security challenges facing the bulk electric system or risk a regulatory response and imposed "solution."

Following the Team and staff introductions, Michael Assante, NERC's Chief Security Officer, offered welcoming remarks and opening comments for the Team's consideration. He noted that this was an unusual standards development process surrounded by an increased level of attention and some sense of urgency. He urged the Team to focus on their standards development task and to take the time necessary to build consensus and answer the critical challenge of coming up with practical solutions that address the directives of FERC and the concerns of the industry. NERC is providing its staff expertise and facilitation assistance to do everything it can to make this effort a success. Mr. Assante also noted the context of President Rick Sergel's recent industry stakeholder letter and congressional testimony highlighting the industry's commitment to making a priority of enhancing security leadership and situational awareness of the urgency of the threat while improving the industry response to cyber security and critical infrastructure protection concerns for the bulk power system in North America.

David Taylor, NERC Manager of Standards Development, reviewed with the Team the need to comply with NERC's Antitrust Guidelines. He then provided an overview of the Cyber Security Order 706 SDT scope, process and roles. Mr. Taylor noted that the 24-member Drafting Team will be responsible for: producing technically sound and complete standard(s) that meets stakeholder and regulatory approval; developing a realistic implementation plan; and preserving the open ANSI process. The Team discussed general comments on the scope, communication networks, serial communications, what should be included in critical assets, comparing NIST and CIP Standards, glossary definitions, bulk power system vs. bulk electric system, responsibility for standards and NERC Standards Development.

Mr. Taylor noted the 24 members of the Team appointed by the Standards Committee will be led by the Chair, Jeri Domingo-Brewer and the Vice Chair, Kevin Perry, who were appointed by the Standards Committee. NERC is committed to providing considerable NERC staff support and expertise as represented by those attending this organizational meeting and by neutral facilitation being provided by a team from Florida State University's FCRC-Consensus Solutions Center.

Bob Jones, with the FCRC Consensus Solutions facilitation team, provided an overview of how consensus could be defined and used by the drafting team as well as meeting ground-rules. He suggested that the Team

agree to the ground-rules and review the consensus process again at the next meeting with an eye towards adopting a procedure going forward.

David Taylor and Gerry Adamski noted that NERC will be developing, in consultation with the Team, a communications effort to the industry to explain what is going on in standards development process so that the industry has a heads up and does not have to digest the entire standards revision in a short period just prior to balloting. NERC would like to see the SDT complete its work within an 18 to 24 month time frame. An FAQ document may be developed by the SDT.

Members discussed who they are serving, i.e. who is the beneficiary, not who does the standards apply to in this process? Is the Congress, the FERC, the auditor, and/or the asset owner? One member suggested the SDT is serving North American society as a whole in working to protect critical infrastructure. The facilitator suggested bringing this back at the next meeting as the SDT reviews, refines and adopts a purpose statement.

The Chair noted that the FERC Order 706 directs NERC to consider the NIST framework. Keith Stouffer, team member and NIST employee, presented an introduction of the NIST approach to standards development to the Team. Stuart Katzke presented on the NIST framework and approach. Marshall Abrams presented a comparison of the NIST and NERC CIP Standards.

Prior to the meeting Scott Mix, Manager of Situation Awareness & Infrastructure Security at NERC, reviewed the FERC Order 706 and created and presented a straw man red-lined version of the CIP standards as an Approach to Phase I issues at the meeting. The facilitator then suggested the Team use the acceptability ranking tool to both test support and focus discussion on a threshold question of whether to proceed with a single phase or more than one phase. The Team ranked and agreed on the following project roadmap proposition: The SDT should proceed with an approach with two or more phases and products for ballot body consideration.

The SDT reviewed and agreed to apply the following draft criteria for consideration of issues to address in Phase-1:

- It represents an "Editorial" item
- It is a must-do item per Order 706 to meet the July 1, 2009 time frame
- It will not preclude the Team changing standards language in Phase 2

The Chair and Vice Chair suggested that the Team review and offer suggestions and concerns with the "straw man" phase 1 proposal that Scott Mix had put together as a "redline" draft of the CIP 002-009 standards in response to FERC Order 706. During the course of the Team's Tuesday afternoon's review of the redline, changes were made to the redline draft. The revised redline draft from Tuesday was then reviewed by the Team and ranked for acceptability and further refined on Wednesday morning. Below is the final draft of the changes in CIP-002-009:

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

CIP-002 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Critical Cyber Asset Identification
A2. Number: CIP-002-~~1~~2
A3. Purpose *(2nd paragraph)*
These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R4. Annual Approval — A senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP 003 — CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

CIP-003 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Security Management Controls
A2. Number: CIP-003-~~1~~2
A3. Purpose *(2nd paragraph)*
Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2. 3Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.~~3~~ 4. The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

CIP-004 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Cyber Security — Personnel & Training
A2. Number: CIP-004-~~1~~2
A3. Purpose:
Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Awareness — The Responsible Entity shall establish, maintain, and document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber security assets receive on-going reinforcement in sound security practices…
R2. Training — The Responsible Entity shall establish, maintain, and document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access. ~~within ninety calendar days of such authorization.~~
R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program prior to ~~within thirty days of~~ such personnel being granted such access.

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

CIP-005 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Electronic Security Perimeter(s)
A2. Number: CIP-005-~~1~~2
A3. Purpose:
Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.

A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009. *(Staff will correct the citations)*

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

CIP-006 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Physical Security of Critical Cyber Assets
A2. Number: CIP-006-~~1~~2
A3. Purpose:
Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1. Physical Security Plan — The Responsible Entity shall create ~~and~~ maintain and implement a physical security plan, approved by the ~~a~~ senior manager or delegate(s) that shall address, at a minimum, the following:
R1.2. Processes to identify all access points through each Physical Security Perimeter and implement measures to control entry at those access points.
R1.4. Procedures for and the implementation of the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
R1.6. Procedures for and implementation of escorted access within the physical security perimeter of personnel not authorized for unescorted access.
R1.7. Process for updating the physical security plan within ~~ninety~~ thirty calendar days of implementation of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement Standard CIP-009. *(Staff will correct the citations)*

CIP 007 SYSTEMS SECURITY MANAGEMENT

CIP-007 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Systems Security Management
A2. Number: CIP-007-~~1~~2
A3. Purpose:
Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Ports and Services — The Responsible Entity shall establish and document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish, ~~and~~ document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches…
R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure. ~~or an acceptance of risk~~.
R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~ thirty calendar days of the change being completed.

CIP 008 INCIDENT RESPONSE & REPORTING

CIP-008 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Incident Reporting and Response Planning
A2. Number: CIP-008-~~1~~2
A3. Purpose:
Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident Response plan shall address, at a minimum…
R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~ thirty calendar days of any changes.
R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

CIP 009 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

CIP-009 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets
A2. Number: CIP-009-~~1~~2
A3. Purpose:
Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~ thirty calendar days of the change being completed.

On Wednesday morning, the Team engaged in a brief exercise to highlight the members' individual preferences for problem solving and decision making. Finally the Team reviewed and agreed to the Phase 1 meeting schedule (both in-person and Webex conference call drafting meetings) and drafting assignments. At the conclusion of the meeting, the Team offered an evaluation of the process including what worked and what could be improved. *The meeting adjourned at Noon on Wednesday October 8, 2008*.

Cyber Security Order 706 Standard Drafting Team

DRAFT ORGANIZATIONAL MEETING SUMMARY

A. INTRODUCTIONS, AGENDA REVIEW AND WELCOMING REMARKS

The Chair, and Vice Chair welcomed the members and asked NERC staff Harry Tom to conduct a roll call of members and participants in the room and on the conference call *(See appendix #3*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

Team Members introduced themselves highlighting a broad spectrum of expertise and industry and governmental perspectives and a shared expectation that they would keep the needs of the industry in mind, but do the right thing. Several noted the importance of engaging and involving Canada in the standards development process. Others pointed to the fact the industry must successfully respond to the cyber security challenges facing the bulk electric system or risk a regulatory response and imposed "solution." In addition, several Team members noted their participation on the first CIP drafting team.

Following the Team and staff introductions, Michael Assante, NERC's Chief Security Officer, offered welcoming remarks and opening comments for the Team's consideration. He noted that he joined NERC as the new Chief Security Officer in September, 2008, moving from Idaho and the Department of Energy's Idaho National Labs (INL) in the fields of security and infrastructure protection to Princeton. He noted prior to his work with INL he served as Chief Security Officer at American Electric Power. Overseeing NERC's plan, at the Electric Reliability Organization, to improve response to cyber and critical infrastructure protection, he noted he will lead the effort in establishing a new core Critical Infrastructure Program at NERC including the critical task of related standards development and compliance.

He noted that this was an unusual standards development process surrounded by an increased level of attention and some sense of urgency. He urged the Team to focus on their standards development task and to take the time necessary to build consensus and answer the critical challenge of coming up with practical solutions that address the directives of FERC and the concerns of the industry. He noted that the Team will not be following someone's model, since no sector has taken this standards issue on. The Team needs to focus on producing just and reasonable standards that are not unduly discriminatory or preferential and that are in the public interest. NERC is providing its staff expertise and facilitation assistance to do everything it can to make this effort a success.

Mr. Assante also noted the context of President Rick Sergel's recent industry stakeholder letter and congressional testimony highlighting the industry's commitment to making a priority of enhancing security leadership and situational awareness of the urgency of the threat while improving the industry response to cyber security and critical infrastructure protection concerns for the bulk power system in North America. The leaders in the sector believe we have a great "culture of compliance" and that the ERO is about achieving real security. He noted that cyber security is a fast evolving area in terms of tools and approaches where there needs to be a balancing of the security value with establishing good measurable standards in a dynamic system. The experience with the Maritime

Security Act of 2002 highlights what lack of flexibility can produce. NERC's hope is to strengthen the regime to protect assets and demonstrate a confidence and willingness to do this right.

Mr. Assante suggested the Team should consider as part of its scope:

- The merits of blackout report recommendations;
- "Must do's" in the short term;
- Eliminate reasonable business judgment in the standards
- How to address acceptance of risk exceptions and accountability.
- Develop specific conditions that a reasonable entity must satisfy to invoke the "technical feasibility" exception;
- Data as a critical cyber asset and help to defining critical assets- and what external review and procedures may be involved and who should be involved in that process;
- Application of a measurable "defense in depth" to create an electronic security perimeter. Different definitions by different world- network view of the world vs. operations.
- What strong controls are needed and how much change triggers an "active vulnerability assessment" (change controls).
- What is a representative system that will allow you to say the testing is enough.
- Security standards and operations realities different, E.g. "resilience," efficiency is the evil to resilience? Philosophically how to protect assets and how to best operate to get to reliability.
- Timetable- One hard date in FERC Order 706 is to remove "using reasonable business judgment" before the compliance audits commence in July, 2009.
- Satisfy what needs to be done in the short term while taking the longer view in the standards development. Are there approaches that might allow addressing important issues sooner?

Finally, Mr. Assante noted that everything the Team will do will be part of an open process guided by the ANSI framework and procedures and, "If we get this right, we can provide a model for the industry and that others can utilize."

B. REVIEW OF ANTITRUST GUIDELINES

David Taylor, NERC Manager of Standards Development, reviewed with the Team 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 these as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive in nature.

C. SDT PROJECT PROCESS, SCOPE, ROLES AND CONSENSUS GUIDELINES

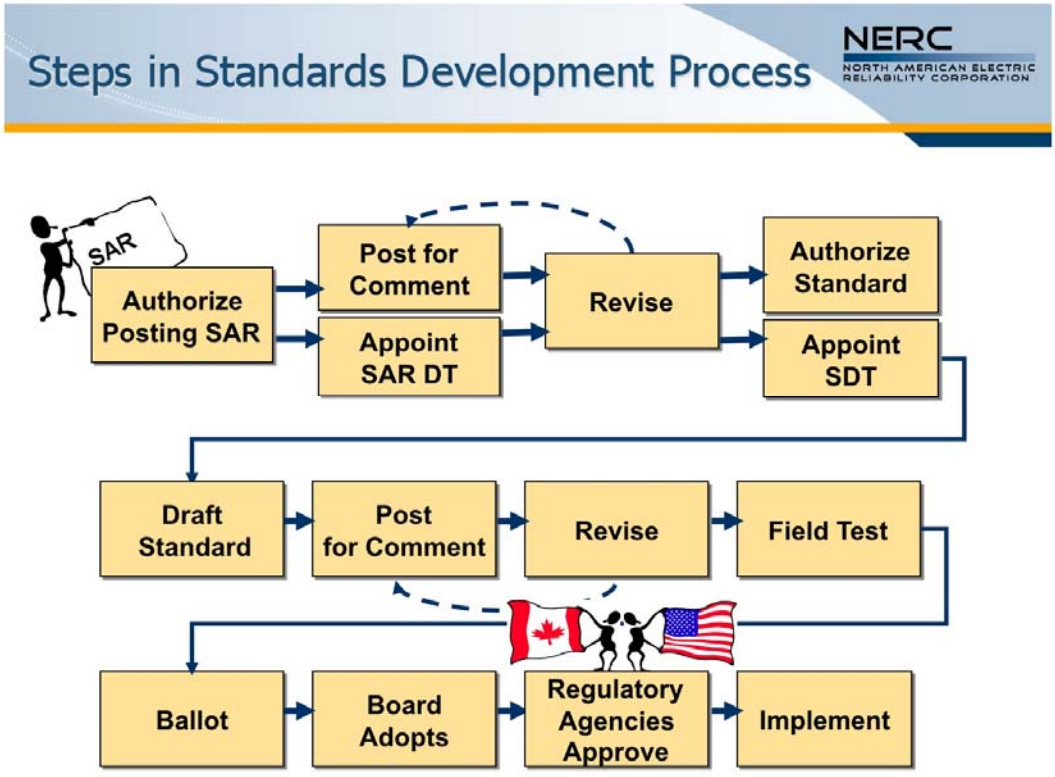
David Taylor, Manager of Standards Development at NERC, provided an overview of the SDT Project scope, process and roles. (See, power point presentation at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

1. Standards Development Process and SAR Scope

Mr. Taylor reviewed with the Team the development and adoption of the Standard Authorization Request (SAR), Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009, June 9, 2008) (See, http://www.nerc.com/docs/standards/sar/SAR_Modify_CIP_Stds_D2_clean_07Jul08.pdf . He noted that the Standards Committee appointed the Standards Drafting Team with an eye towards member expertise and representation of both geographic and industry segment perspectives. The 24-member Drafting Team will be responsible for:

- Producing technically sound and complete standard(s) that meets stakeholder and regulatory approval;
- Producing a realistic implementation plan; and
- Preserving the open ANSI process.

He described the potential phases of a standards development process featured in the graphic below:



Mr. Taylor noted that if there is anything that needs to be changed in the standard, the group should raise the issue. Historically SARs have been narrowly focused. He noted that Volume #1 of Standards Development Plan outlines that the scope of the standards

development process and directs teams to effectively deal with standards overall to produce an effective standard. Taylor expects the majority of the time to be spent on Requirements and on accompanying Measures. In the past the requirements may not have been written to provide clarity. David Taylor and Maureen Long of NERC will review the Team's products for completeness and clarity prior to posting. If the requirements are not clear, modification will be required. All requirements must be measurable. If the requirement cannot be clearly measured, then the drafting team will be asked to re-write the requirement and measure. The measures must be precise and understandable by both the entities and the auditors.

The drafting team should address all the issues identified in the Issues Database prior to posting and the standard should meet NERC benchmarks for reliability standards. The expectation is that each of the existing requirements and modifications and an implementation plan should be addressed and the drafting team will be expected to respond to all comments. He noted that the Team will need to decide fairly early on if they are going to address something with a revision to the standard or address a FERC directive via external guidance documents.

Mr. Taylor addressed the following SDT Scope items:

Balloting and Implementation
- What is directed in Order 706
- There is a spreadsheet that lists the items in Order 706 to be addressed by the drafting team.
- Determine the optimal implementation plan

Clarify Existing Requirements
- Consider the need for different requirements for different environments, i.e., control centers, substations, generation, etc.

Other items including interpretations.
- The team may believe it should consider clarifying interpretations, etc.
- E.g., Within an ESP, the wiring over which data flows should be protected.
- E.g., Application of CIP to Nuclear

Industry education
- FAQ document revision/replacement
- Development of guideline documents such as those for extended LAN's over multiple geographically dispersed locations

Finally, he noted the following products that must accompany a standard change and are used by the NERC compliance staff:

- A standards requirements document (saying what the entity shall do but not how they do it).
- An SDT Implementation Plan for the Standard(s)
- A Comment Form which presents an opportunity for the Team to tell the "story" behind the proposed standard and asks some very pointed questions for industry to respond to in providing input.

- A document describing Violation Risk Factors –focusing on Severity of impact and are used by auditors to determine, along with other mitigating factors, the initial sanction "price point."
- A document describing the Violation Severity Level — i.e. how badly off from the compliance mark was the entity being audited? This will expand on the measure. Note that VSLs were not a part of the original CIP standard development, instead there was a separate team working on initial VSL. This team will revise VSLs as part of its process.

Finally, Mr. Taylor noted the following reference documents that had been sent in advance to the Team:

- Reliability Standards Development Plan — Volume I
- Reliability Standards Development Procedure
- Standard Drafting Team Guidelines — the SDT bible
- Pages 7–11 of the SAR gives a lot of really good information.

Team Member Comments and Questions on SAR Scope

- **General Comments on Scope**

- Extended WAN — consider Ethernet Over SONET.
- Consider the impact of Smart Grid (AMI, etc.).
- Try to stand back and look at the bigger picture.
- The word "etc." in the requirement to consider other information sources is believed to give the SDT the latitude to go wherever it needs to.
- Need to be more explicit where the ESP begins and ends.
- Need to be cognizant of the use of high speed communication and cost models.
- Need to look at CIP-002, including the RAWG guideline and the NIST framework. Does not mean we throw out the CIP standards and wholesale replace them with the NIST standards.
- Perhaps there is a minimum set of requirements that apply to all cyber assets and an elevated set of requirements that apply to critical cyber assets. The NIST/FISMA risk framework gives you this latitude.
- The fear is the threat of financial sanctions. That is the big roadblock against moving away from the existing cherry-pick approach.
- The RAWG guideline looks at the problem from a functional perspective (generation, transmission, systems, and special controls). The CIP-002 as it exists today does not organize the same way.
- Verizon data breach study — victims are not taking upstream/downstream connections seriously. No longer a predominately internal threat.
- Is everything fair game as far as the SAR is concerned? Answer: There is an item in the SAR that provides freedom to include other related items as appropriate.

- Are **Communication networks** today out of scope in terms of the SAR? Answer: If the communications are disrupted via the end points, such as the meters, the

question of who is responsible is not clear under today's standards. The communications provider is not responsible. Issues similar to this should be within the scope under "other items". However, the standards drafting team will probably not have authority to decide this issue.

- **Serial Communications**: a strategy of moving IP based systems away from IP communications and back to serial communications by some industry participants may not be a good idea. FERC intends to address this issue in the future.
- **What should be included in Critical Asset?** Could the definition of Critical Asset be expanded to cover a broader set of reliability standards? The answer is yes, it is within scope of the SDT. RAWG is leading the process of developing a guideline for Critical Asset identification in support of the existing CIP standard. Jay Cribb, chair of the RAWG and member of this Team can be a conduit between this drafting team and the work of the RAWG.
- **NIST and CIP Standards.** Federal strategy is to try to adapt existing NIST standards to new environments. For example, applicability of SP 800-53 to control systems. Very difficult to apply. Added additional information to a good number of 800-53 requirements to specifically apply to control systems (Became SP 800-53, Rev 2). We can learn from the NIST experience. NIST will provide as little or as much detail and assistance as the SDT wants. NIST 800-39 provides some directives. NIST 800-39 should be looked at very closely because we have been directed to do so and because it makes sense when studied. We may not be able to provide cyber security protection of the systems that support the electric grid using the Critical Asset directives contained in CIP 002. The drafting team should be free to replace CIP 002 with the NIST framework if they determine this is the right course of action. NIST 800-39 may provide a framework that can be used over time. Based on risk, there are different levels of security that may be applied to different assets at different levels of risk.
- **Glossary Definitions.** Definitions that are global to NERC, how does the drafting team work with them? Answer: NERC Glossary terms used in standards are capitalized. All glossary terms must be universal and not specific only to the cyber security context. Changing the way a word is defined in the NERC glossary could have a ripple effect throughout other standards where the word is referenced. If it is in the NERC glossary, that is the definition the drafting team should use or propose a change to the glossary. The drafting team may want to propose that new definitions are added to the glossary.
- **Bulk power system vs. bulk electric system.** The terms "bulk power system" and "bulk electric system" may be contingent upon the regional definitions. What term will the Team use? Answer: BES will be used until further direction is provided by FERC. BPS is more expansive than BES, but FERC did not probably expect imminent compliance across industry. FERC expects eventually that all the NERC standards will apply to the BPS and not just to the BES.
- **Responsibility for Standards.** Who is responsible for published standards? Answer: NERC is responsible in conjunction with the industry for ERO standards. NIST is responsible for publishing their standards.

- **NERC Standard Development**. Will or can we limit the number of revisions? Answer: Based on experiences to date, the Team should expect 2 or 3 drafts in responding to comments. The plan is have a good idea of what the industry wants prior to submitting the standards for ballot. Can the standards be separated or do they need to be balloted as a group? Answer: This is part of the road map for development. This question will be decided over the next couple of days. The ballot body is not typically expert in cyber security matters and companies will turn to their experts for guidance. Is this process of 18 to 24 months soon enough to satisfy the regulators? Answer: NERC's responsibility is to assist the group. There is urgency but CSO's role is to assure reasonable expectations. The Team should have time to 'get it right.'

2. Roles in the SDT Process

Mr. Taylor noted the 24 members of the Team appointed by the Standards Committee will be led by the Chair, Jeri Domingo-Brewer and the Vice Chair, Kevin Perry, who were appointed by the Standards Committee. NERC is committed to providing considerable NERC staff support and expertise as represented by those attending this organizational meeting and by neutral facilitation being provided by a team from Florida State University's FCRC-Consensus Solutions Center.

3. Proposed SDT Consensus Guidelines and Meeting Ground Rules

Bob Jones, with the FCRC Consensus Solutions facilitation team, provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6)*. He noted that consensus can be understood as having three meanings in a group process: it is an attitude of each of the team members, it is an outcome or decision rule for the team, and it is a structured problem solving process. He suggested that the Team has some flexibility to define what a 'consensus' decision should mean for the Team's process. He noted that among the ballot body, a standard requires at least a 2/3 majority of all of the industry segments to be adopted. The Team may want to establish a higher supermajority for agreement (perhaps +75%) to assure 2/3 acceptance of the ballot body. He suggested that this could serve as a default standard and that the process would be designed to seek 100% acceptance of the Team. He suggested that the Team review this again at the next meeting with an eye towards adopting a procedure going forward.

Mr. Jones proposed a set of ground rules for the meeting. *(See, Appendix #6)*.

Team Comments on Ground rules

- Perhaps some additional phone protocols
- Say your name at the start if you are on the phone — "comment on the phone" with name to get in the queue to speak on an issue
- Check with team members on the phone to include their acceptability ranking as needed
- In past group this large need to clearly state what we are trying to get consensus on to aid in staying on issue and avoid drift

4. Expectations of Drafting Team

David Taylor and Gerry Adamski noted that NERC will be developing, in consultation with the Team, a communications effort to the industry to explain what is going on in standards development process so that the industry has a heads up and does not have to digest the entire standards revision in a short period just prior to balloting. NERC would like to see the SDT complete its work within an 18 to 24 month time frame. An FAQ document may be developed by the SDT.

Members discussed who they are serving, i.e. who is the beneficiary, not who do the standards apply to in this process? Is the Congress, the FERC, the auditor, and/or the asset owner? One member suggested the SDT is serving North American society as a whole in working to protect critical infrastructure. The facilitator suggested bringing this back at the next meeting as the SDT reviews, refines and adopts a purpose statement.

D. REVIEWING THE NIST FRAMEWORK AND COMPARISON WITH THE NERC CIP STANDARDS (002-009)

The Chair noted that the FERC Order 706 directs NERC to consider the NIST framework.

1. NIST Framework

Keith Stouffer, team member and NIST employee, presented an introduction of the NIST approach to standards development to the Team. He noted that he does not believe a wholesale swap out of NIST for the CIP is prudent, but he believes there is quite a bit to be gained for the SDT in reviewing the NIST approach. He noted that the NIST strategy has been to look to see if they can add additional guidance to their framework to support applications such as control systems environment. The first thing they looked at was 800-53 requirements by bringing stakeholders together to determine what concerns exist. They determined 800-53 as written would not apply well to control systems so they created a Revision #2 to 800-53 for entities which operate control systems and must comply with NIST requirements. Keith noted that NIST is ready to help as much or as little as the drafting team wants. NIST provides an alternative way of looking at the standards.

Keith Stouffer then reviewed a presentation that he gave to the NERC Standards Committee. His power point presentation is available for review at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html. Key points in Keith's presentation included:

- NIST keeps measurement standards, but they also create principle-based standards.
- 800 series contains information systems guidelines. Auditing done by GAO. There are about 115 of the 800 series documents.
- FIPS — standards approved by the Secretary of Commerce.

- NIST 800 documents go through a 3 stage public vetting process, but do not require Secretary of Commerce's approval.
- Connection between FIPS and 800 documents includes a reference in FIPS to the 800 series documents. Therefore a change in a reference in FIPS to an 800 series document does not require Secretary of Commerce's approval.
- NIST approach to Standards Development in order of priority
- Seek commercial sector involvement and attempt to adapt an existing document.
- Review other existing standards to see if one of those can be adopted.
- Create a new document.
- 800-53 is the document used for securing Federal information systems.
- Over 800 comments received on the initial public draft
- In response NIST streamlined the controls
- Revised in 2006 and again to revise for control systems in late 2007.
- NIST brought in industry companies covered by 800-53 and determined why implementing the controls created problems for the companies covered by the document.
- There are 3 levels assessed for each control. For example, for a system categorized as low the particular control may not apply or only parts of the control may apply.
- 800-53 cannot be used for both general information systems and control systems.
- The following framework allows the organization to tailor the controls to their systems:
  - Low Impact: Selection of a subset of security controls – Non hazardous materials
  - Moderate builds a low baseline. Selection of subset of control from the master catalog – Some hazardous material & some proprietary information
  - High Impact: Highest level - Protect human life
- Federal Government approach
- Use the existing NIST risk framework
- Make modifications
- Apply to control systems
- 800-82 provides guidance on how to implement 800-53.
- Final public draft released in September of 2008 with 60 days for comments
- Used in the private sector for control systems

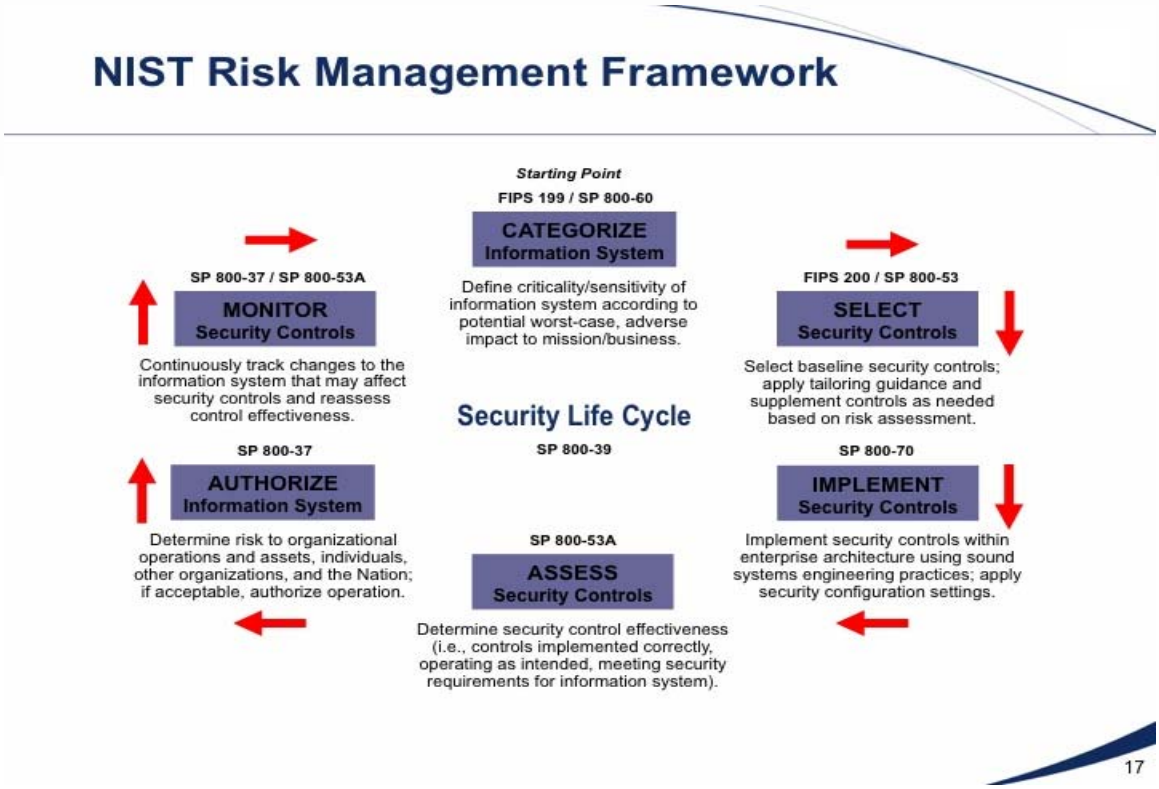
Stuart Katzke presented on the NIST framework and approach, (see, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html) including the following key points:

- Control mapping was the easy part. Harder part was looking at model and the underlying model for CIPs.
- NIST is a "Plug and play" framework-
- FIPS and 800 documents — are security standards and guidelines.
- Tasked under FISMA to do 3 things:
  - Categorization scheme for info and info systems;
  - Guidelines for categorization;
  - Create minimum standards for categories.
- 3 buckets- low, mod, high based on worst case impacts and decide which bucket.
- Minimums imply more is required. Not a good 1 size fits all solution.

- Put flexibility in standard by fixing the standard and have the guideline allow you to tailor it.
- Look for ways to compensate.
- Minimum control smacks of a compliance/regulatory view. Inclined toward understand and accept risks.
- When system is ready to go- controls will be in place and operating. This goes into authorization to operate (accreditation) decision.
- Certification- assessment of security controls
- Problem- evolved into a paper work exercise — boon for consultants.
- Accreditation/certification woven into the process vs. an end checkpoint.

Team and Participant Comments on the Presentations

- NIST approach includes understanding risks under assessment and the intent of the controls. If the controls cannot be implemented, the users must understand the intent of what the control is trying to accomplish and implement controls which compensate for the intent of the control which will not be implemented.
- NIST approach includes continually assessing level of security. Therefore, following the NIST model correctly will result in being in compliance.
- The framework of NIST occurs within the information system development lifecycle. Today's CIP standards apply to Critical Assets, which may include control centers, generation plants, and substations.
- 800-39 presents a broader view for inter-connected information systems and external entities.
- 800-53 sets standards but doesn't tell how.
- Reviewed all controls. Provide guidance re problems in applying controls to this environment.
- 17 control families; 171 controls (requirements).
- Control enhancement to original control. Low/Mod/High. Based on level of impacts if system is compromised. Additional rigor as you go up to high.
- 800-53 took about 1 year to develop draft.



- NIST Risk Management Framework/Security Lifecycle
  - FIPS 199/800-60 — Categorize information Systems (low, medium, high)
  - Level of rigor is based on the categorization
  - FIPS 200/800-53 — Select Security controls
  - SP 800-70 — Implement Security controls
  - SP 800-53A — Assess Security Controls
  - Security Assessment plan is required & independent assessor is required for moderate and high impact systems
  - SP 800-37 — Authorize Information System
  - SP 800-37/SP 800-53A — Monitor Security State
- NIST does not perform the assessments or audits. NIST gets feedback from the GAO surrounding changes that may be required to NIST standards.
  Merging systems together- depends on circumstances.
- Assess controls when a security event occurs.
- How does system hold up to scrutiny — NIST relatively new.
- Look at control sets following events —
- Would the BES need an organization to manage family of controls, to assess etc.?
- GAO reports on incidents.
- Consider Total cost of ownership — with a life cycle framework approach. Need to think through the care and feeding.

- Assessment based upon what the org decided are its goals in an area. Measurable and $$. Tendency to shoot low. What are they assessed against for standards. How to encourage how to set their goals high.
- Assessment against controls vs. goals? Assess security controls- audit focusing on $$. Adopt lower level of controls.
- Adequately secure vs. meeting controls.

Team and Participant Comments on the NIST Framework

- For control system how are federal agencies categorizing systems- which baselines using? FIPS 199.
- Assignment clause — organization defined list of inappropriate or unusual activities that are to result in alerts? The organization determines within the framework of control.
- "regularly reviews" -organization determines the frequency.
- CIP standards — for not keeping 1 document up to date is a potential violation that is not consequential to security. Evaluating the level of control vs. small pieces = violation.
- NOPR in 706- might provide too much angst.
- Compliance elements- onerous.
- "If it ain't written down, it didn't happen."- This captures the old view.
- If we go down more prescriptive route- have to clarify the costs of putting this in place. Intensive to implement controls.
- Tell me exactly what I have to do. Flexibility factor is providing
- Control and enhancements. Low mod high — lots of variation.
- Changes- didn't change any of the controls in 800-53. Instead provided additional guidance to 645 of 171 controls to address ICS (industrial control systems)
- Control systems- not all in BES context.
- DOD interested in this approach — now they use their own.
- 882 supplemental- security process controls — 800-53 revision 2 is requirement
- Security baselines- low, mod, high.
- 800-53- tailoring baseline security controls to fit needs.
- Industrial control systems security guide
- 800-82- Sept 08 final public draft. Out by end of the year.
- 90% of ICS are industry.
- ISA 99- Bryan Singer. ANSI — Industrial Automation and Control Equipment
- IEC 62443- Tom Phinney.
- Not just compliant – compliance with baseline does not equal security.
- Must define minimums.
- Life cycle management? Not a maturity element. Degrees of rigor come in depending on impact level.
- One large interconnected system- what is the system? Each separate or one?
- What is the info system (accreditation boundary- what you have control over)
- NIST Protecting info systems. CIP speaks to critical cyber assets and non-critical not necessarily systems. Apply all the CIPs.

- Framework- differences- NIST- system level approach requires high degree of system/state awareness of context of components. CIP – make judgment about critical assets and apply approach.
- Accreditation boundary — are we Industrial control systems or not?
- Draw boundary around set of components and consider as a holistic system.
- Evolved to enterprise wide view of activities. (mission, role, impacts on organizations and other depending on organization.
- Information system: accreditation boundary- components within- people, processes and technical- management operational and technical controls.
- "Common controls"-training, physical security) provided to system from external sources.
- NERC standards- cyber security not factored into overall trainers as a common control. Should be doing this going forward. Operators are first line of defense.
- Assignment of responsibility- asset/system owner. Where does responsibility lie that everyone getting access to critical asset is properly trained?
- Flexibility to flavor requirements specific to each environment within organization.
- CIP- accountable executive- responsibility assigned. It is there? Yes but not as prescriptive as NIST standards. Needs to be open enough, not too prescriptive. Split into different number because ANSI. Not being read as one standard.
- ESP boundary in CIPS vs. the NIST boundary and everything within.

2. Comparison of NIST and NERC Cyber Standards

Marshall Abrams presented a comparison of the NIST and NERC CIP Standards. (See, his PowerPoint presentation at: http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

He noted both the similarities between CIP vs. NIST (e.g. concepts of internal/exterior boundaries, etc.) and the differences between CIP vs. NIST (e.g. NIST uses information system view rather than NERC Critical Asset/CCA view, NIST allows holistic defense in depth approach through system design, etc.) Other points included:

- Under CIP security requirements are applied to all components whether the components are capable of supporting the security requirements or not (i.e., legacy substation devices);
- Under CIP Treating boundary and contents separately (CIP 005 and 007) creates problems;
- Wireless is addressed in NIST but not in CIP.

Mr. Abrams handed out a NIST augmented CIP and NIST Example of Augmentation of CIP 005. See, http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

Team Discussion of NIST compared with the NERC CIP:

- NIST staff performed the mapping of the CIP vs. the NIST standards to assist Federal entities which had to comply with both NIST and CIP.

- CIP 002-009 standards should be taken as a whole and that many of the concerns which have been raised can be answered in either one of the other CIP standards or in the CIP FAQ.
- The Chair and Vice Chair reminded the Team that they have an obligation to set aside partisan opinions of whether members support NIST or CIP but to do the right thing for enhancement of cyber security standards.
- A mapping of what is? Indicates controls or part of controls added CIP requirements.
- Gap assessment- e.g. Least Privilege- mapped to 007?
- Identification and authentication- not adequately address to CIP.
- Configuration management- adequate records/documentation, who can make change.
- Auditing and accountability- e.g. time stamps missing?
- Risk Assessment- R4 renamed- vulnerability assessment and testing.
- System and Communication protection
- Certification, accreditation.- CIP examining controls, managing as intended.
- Security assessment suggestions: security assessment requirement- Responsible entity
- This is not easy. It is on 007.
- Forced by ANSI process. All 1300 were one standard. Read as one standard 2-9.
- Are ANSI rules being cited correctly?
- Technical feasibility with an exception process.
- Suggest level of review- exception plan. Annual audit compliance.
- Physical security?
- CIP Standards- 002-009 should be read as one. It is stated in each in the purpose statement.
- What value might this add- square peg through round hole?
- Let's not spend our time defending the CIP standards.
- Size and risk aren't correlated in CIP?
- Restrict access- assess risk posture of business partners.
- Not try to defend but point out where it was taken care of in the standard.
- Lots of things we need to fix. Gives options to fix few things.
- Procedures written by each company is where NIST and CIP standards come together.
- E.g. "reference we are meeting NIST standard to meet CIP requirements."
- Look at comparison paper on NIST website- Marshall et al.
- Red guide- restricted distribution. Undergoing future review and modification.
- NIST standard has more specificity in all areas. What has to be done not how to do it.
- Team has an opportunity to do what is right. Re-write, incorporate as much or little of 800 framework. Set aside love of one or other. What do we need to do to achieve the goal. This should not be about pleasing auditor or pleasing FERC, but about improving security of the BES for benefit for North America.

E. REVIEW OF HOW TO STRUCTURE THE SDT PROJECT ROADMAP

1. Initial Overview of "Straw Man" Multi-Phased Approach

Prior to the meeting Scott Mix, Manager of Situation Awareness & Infrastructure Security at NERC, reviewed the FERC Order 706 and created and presented a straw man red-lined version of the CIP standards as an Approach to Phase I issues at the meeting. The facilitator then suggested the Team

use the acceptability ranking tool to both test support and focus discussion on a threshold question of whether to proceed with a single phase or more than one phase. The Team ranked and agreed on the following project roadmap proposition: The SDT should proceed with an approach with two or more phases and products for ballot body consideration. (*See, power point, "Cyber Security Standards: Development Proposal at)*. His key points included:

- Violation Severity Level process is beginning for all requirements
- The only date-certain in FERC Order 706 is for the required change is removal of " using reasonable business judgment" by end of June 2009.
- NERC is developing training for NERC regional compliance auditor staff on CIP
- Meeting frequency for the Team- may have to meet face to face every other week for 2 to 3 days
- Proposing 3 phases with doing the "easier" and "must do" work first:

  1. Low hanging fruit — high priority — Reasonable business judgment needs to be removed
  - Complete & to Commission in 6 months (March of 2009)
  - Mostly non-contentious issues
  - NER staff has a proposal of these items

  2. Moderate/Majority of issues
  - Complete and to the Commission 18 months following #1 (October of 2010)

  3. Large challenging, complex, controversial issues — Take a long time to get through
  - Following #2 above – exact timing depends on how many and how long
  - Extremely large and challenging issues.

- Guidelines need to be addressed. Guidelines are NOT standards and are NOT requirements. Cannot be sanctioned for not following a guideline. This drafting teams needs to determine whether a topic needs to be addressed in the standard or in a guideline. CIPC is ready to write guidelines. The Team needs to identify what needs to be done and whether or not CIPC needs to be the writer. About 25 guideline topics have been identified in the FERC Order 706. What can be started now because the subject requirement is not expected to change?
- Develop modification to standards language
- Develop Violation Risk Factor/Violation Severity Level
- Develop implementation timeline and effective date — Less complicated
- Industry review and comment
- Industry ballot
- BOT Approval
- Submit to FERC prior to spring of 2009 and prior to the beginning of CIP audits.

Scott then reviewed a red-lined straw man draft for the Team's consideration that included:

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION
Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Newly identified Critical Assets was put into the parking lot.
- Annual approval by Sr. Manager of the Risk Based Assessment in addition to the CA list

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Slight modification to the specifics requested for the designated senior manager

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- The individuals shall be trained prior to being granted access rather than within 90 days of access
- Individuals shall be background screened prior to being granted access rather than within 30 days of access

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Minor editorial changes only

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Several items where the word 'implement' was added to clarify that requirements must be both documented and implemented
- Item concerning the fact that dial up accessible CCA's using dial up only do not require physical security was put onto parking lot

CIP 007- SYSTEMS SECURITY MANAGEMENT

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Removed acceptance of risk from Malicious Software Prevention (R4.1).
- Added implement under R7 Asset disposal or Redeployment.
- Editing to cite revision number
- Document maintenance was changed from review in 90 days to review documents within 30 of changes

CIP 008- INCIDENT RESPONSE & REPORTING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Added implement when necessary to R1
- Added that testing the Cyber Security Plan does not require taking the component out of service.

CIP 009- RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Proposed language changes include

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.

- Changes must be incorporated into the plan within 30 days of the change

2. Discussion of More than One Phase

The facilitator suggested the Team use the acceptability ranking tool to test support and identify issues on a threshold question of whether to proceed with a single phase or more than one phase.

Team Clarifying Questions:

- Need to see what is "low-hanging" to see if time frame works or not
- Why the spring deadline? See, Letter of Response from NERC President Rick Sergel.
- Do we have to wait for the beginning of a phase to begin addressing the issue identified for that phase? No, can work on some key issues for phase two during the first phase while waiting on balloting for example
- CIP2 — concept of critical asset based assessment (NIST) versus security approach (NERC – CIP)? If tackle that then could look at current standards. The low-hanging could improve some of the current standards. If change course then earlier the better. Address some of the issues and standards before then. An incremental change over what we have now.
- If something is put up for ballot, does that preclude changes that impact it later? Identify and address first phase then address additional issues. Do not want to readdress issues a second time in phase two. Creates confusion and doubt in the industry.
- Concern is with phase two — put off more complex issue to third phase there the danger increases for addressing issues twice
- What happens in first ballot and someone votes no but it is not anything we thought about changing, is irrelevant to modifications in the ballot? There are no provisions against that happening. ANSI offers opportunities to address but upfront. Other bodies have provision saying you cannot object to something not in the proposed revision.
- Clarifying that phase one is low contention and easy and everything else is pushed to future phase(s)
- If it is in phase one does it impact the audits starting next July? Could establish a tiered approach to implementation of items in Phase One to address this.
- Only alternative is one monolithic approach rather than this proposal to break it up.
- Yes, but the "reasonable business" standard would still need to be removed by next July no matter which approach

***Roadmap Strawman Proposition*:**
"The SDT should proceed with an approach with two or more phases and products for ballot body consideration."
(This proposition does not identify what might be in each phase, just that there can be multiple phases. If a multi-phased approach is not adopted, then the approach would be that all standards changes are made within a single phase.)

First Poll on	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable*	*1 — Not acceptab*

More than 1 phase			*if major issues are addressed*	
Avg.=3.4	**11**	**8**	**2**	**0**

Team Comments following the First Ranking

- *2 ranking*-at least two items proposed for first phase concern me — first phase include easy ones but reasonable business standard needs to be deleted and then addressed in the next phase
- *2 ranking*. It is intuitive that low hanging fruit like the reasonable business exceptions language should be separated from this group while this we tackles tougher issues. However dealing with "low hanging fruit" in first phase may signal to the industry that the current standards are generally fine and we may encounter resistance when we come back to address the phase 2 tough standards issues.
- Would it be possible to address the FERC "reasonable business exception" issue and low hanging separately outside this group? Could NERC address the reasonable business standard separately? Alternates to this committee? Not given the approved SAR assigns this to the Team.
- *3 ranking*. Timetable for phase one is a concern — need more time, can we ask for an April, 2009 vs. March, 2009 deadline?
- *3 ranking*. Support a two phase but not four phase effort.
- FERC said "you must remove" and then President Rick Sergel committed getting something done quickly to be responsive to those with oversight.
- Can you just send out an advisory note saying the reasonable business judgment is no longer valid? Not appropriate to make such a statement outside the drafting process – some immediacy emergency alert exceptions to close gaps in a short order and it is not an action order, not super-ceding an existing standard as indicated here
- Another way to deal with? Issue a separate SAR and standard with red-line striping it out for comment

Following the comments and discussions regarding concerns revealed in the first poll, the Team ranked the same proposition with the following result.

Second Poll on More than 1 phase	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptab*
Avg.=3.5	**14**	**5**	**3**	**0**

The Chair suggested that SDT should review and seek to agree on identifying "low hanging fruit" and must do propositions for early comments and ballot testing. The Vice Chair suggested that the question is not how many phases should there be, rather how to separate out those issues which can be quickly resolved from those items which require a longer time for resolution.

3. Draft Criteria for Inclusion of Issues in Phase-1 Product(s)

The Facilitator proposed draft criteria for inclusion of issues in Phase 1 for the Team's consideration and refinement:

- **It represents an "Editorial" item**

- **It is a must-do item per Order 706 to meet the July 1, 2009 time frame**
- **It will not preclude the Team changing standards language in Phase 2**

==========

- ~~Clarification item to design and implementation~~
- ~~Little known industry resistance~~
- ~~Limited complexity~~
- ~~Builds confidence~~
- ~~Correct known or obvious deficiencies~~

Team Comments on Draft Criteria

- "Clarification item"? I may not be able to live with this – too broad. May turn an FAQ into a guideline.
- Drop the "builds confidence" — I would say correct known or obvious deficiencies
- Correct known or obvious deficiencies (**I cannot live with this — too broad**)
- Builds confidence (** How measured? ** — just a reason for doing)
- I would add after third bullet "per 706" — that handles efficiency, drop the rest of the list as political optics — first three enough
- "Clarification" could still be very contentious
- "Building confidence"? do not know which those are?
- Okay with simple edit and per 706 must do removal of reasonable business standard
- The more we put in then the tougher it is to do it quickly
- Editing and must do should be included
- "Clarification" is just change 'design and implementation'? The "that is what we meant last time" items
- Removal of Reasonable Business Judgment, coupled with leaving some other things in that FERC wants addressed, will give the entities some latitude.
- Will FERC reject the phase 1 revisions because not everything else has been addressed? FERC staff will be attending the meetings and reporting back to the Commission on the progress, with a recommendation for approval or not, notwithstanding the fact that there are other changes pending.
- Issue of new CA/CCA does not need to be in the standard. Could possibly be handled via new Implementation plan table.
- Difficulty with the level of this discussion, it feels down in the weeds — expressing what could be in or not in phase one —
- Industry on the whole sees these issues as moving targets. The danger is if we have to go back and readdress an issue it will cause confusion in the industry.

F. PHASE I STRAWMAN REVIEW AND CONSENSUS TESTING- CIP 002-009

The Chair and Vice Chair suggested that the Team review and offer suggestions and concerns with the "strawman" phase 1 proposal that Scott Mix had put together as a "redline" draft of the CIP 002-009 standards in response to FERC Order 706. During the course of Tuesday afternoon's review of the redline draft, changes were made to the redline draft. On Wednesday morning the Team reflected on Tuesday's work and offered the following comments:

- I heard we want to get first piece out and into the process, then take some time with remaining issues — deal with time directive, then take time to look at meat of the problem.
- Is there a risk that we are toothless tiger if there is not enough progress in the first phase — will industry look up and say is that all?
- Extremely short time for change with a time certain — in communication plan must clearly let industry know there is a lot more work to come and just dealing with an immediate issue — do not put a show stopper in that keeps us from getting immediate need done.
- Higher risk to putting too much in than too little — will cause dissension and make us look like we do not know what we are doing.
- Communication plan important — get message out that we will be dealing with tougher issues.
- Two edge sword — hardest part of implementation comes in June — too much in and the industry will ask what are we doing to them — need to address FERC's request
- We say more by saying less in Phase 1.
- Implementation plan for new assets — consider addressing that and it will let industry know we are being responsive
- Go through redlines and test comfort level with what we did yesterday – some can be dealt with as implementation — create a new table 5 for implementation with groups permission and later review and approval.
- Industry may want to make comments on the requirements, measures and implementation plan – if there are controversial issues with the draft, the Team has the option of removing them before balloting.

The revised redline draft from Tuesday was then reviewed by the Team and ranked for acceptability and further refined on Wednesday morning.

OVERALL

Removing Reasonable Business Judgment Language discussion:

- If we remove the references to reasonable business judgment in CIP, what does the drafting team tell the industry they will replace for the phrases that are being removed?
- NERC staff noted there will need to be a communication plan so that the industry understands the changes that are being balloted and why the changes are being made.
- This same type of communication will need to occur at FERC so that FERC does not review the language with the elimination of reasonable business judgment but not approve the new version because it fails to address the bulk of other required changes.

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Newly identified Critical Assets was put into the parking lot.

- Annual approval by Sr. Manager of the Risk Based Assessment in addition to the CA list

Tuesday Comments on 1st Review of the Redline

- "Reasonable business judgment" – just eliminating the end of the sentence or the whole sentence?
- Confusion if leave in the first part of that sentence — eliminate the whole sentence
- Eliminate whole sentence and avoid confusion
- Have to remove it — but must convince ballot body that it has been replaced by something somewhere
- Need supporting discussion as to why — eliminate because FERC asked us to and continuing to address the issue — acknowledge it is a small step in the right direction but only the first step
- Two main issues: based on finance not reliability — better ways to go dealing with risk management in other places in the document — kept "technical feasibility to retain flexibility but explain why
- Rather than just strike and assume dealt with below — struck for legal interpretation – should we still have the flexibility in managing to give industry flexibility without this statement
- We are meeting deadline and continuing to deal with the issue carefully - assurances we are dealing with it
- Application of exceptions must have a plan to address mitigation of the exception
- Suggest keeping both RRO and RE — later as .12

R3 – Critical Asset Identification Review?

- Don't list all the entities
- Take out the word "submit" – shall review
- Thus bump it off and address later
- Put in periodicity

R4 Newly identified critical asset

- Bump it
- Need to address when in compliance once merger takes affect — asset piece is on line — newly identified or acquired asset
- For nuclear folks they will balk at one year — evolving issue of applicability — understanding or grace period for those late to the game —
- This does not address a brand new asset — can be handled through table 5
- Requires more discussion — move it to later
- Handle through additional to implementation table — not the standard
- Cover acquisition as a separate issue?
- Add "acquired"?
- Important to address the issue — impacts when and how to bid on a system — when do I have to bring it into compliance — base line issue
- Put into early phase — phase one — but not today
- Put into phase two — but early in that phase both R4 and R5

Old R4: okay

CIP- 002 Wednesday Morning Rank, Review and Refinement

Poll on CIP 002	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptab.*
Avg.=3.5	**22**	**0**	**1**	**2**

Team and Participant Comments after the Ranking

- Version updates and excise reasonable business issues (for all sections)
- Senior managers approval the only change
- Measures okay but will make change to table at the bottom
- Risk assessments changing next year — need newly identified assets here or somewhere else — comfortable with this going forward if reassured about the proposed implementation table 5 — if abandon from requirements then need somewhere
- Newly identified assets — new definition in glossary? No, put language at top of table
- Newly constructed assets? Can handle within the table but is a different issue

CIP 002 – CRITICAL CYBER ASSET IDENTIFICATION

CIP-002 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Critical Cyber Asset Identification
A2. Number: CIP-002-~~1~~2
A3. Purpose *(2nd paragraph)*
These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R4. Annual Approval — A senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Slight modification to the specifics requested for the designated senior manager

Tuesday Comments on 1st Review of the Redline

- Same issue of "reasonable"

- Same issue of RRO and RE's

R2.1 senior manager clarification

- Use the word fiduciary responsibility
- Can't sue the federal govt.
- Clarifying response to comments received
- "a manager" is just one, not a set of?
- In some cases it is the senior manager of each business unit within the organization
- Defining a single person for compliance when there is a second person responsible for implementation — and the two are not responsible to each other
- Intent is to establish a clear line of authority to give cyber security a higher level of importance — a person with clear line of authority who can delegate authority
- Delegation language down in R2.4
- Any thought given to how it applies in and organization with nuclear and non-nuclear facilities — depends on whether or not each is held out as a separate legal entity — how is the entity registered?
- "Senior manager accountable for"? Language here is quoted from the FERC order
- no opposition to including
- R2.4 establishes the paper trail for delegation — the form for R2.1 should include requirement to list delegation — "documented in the same manner as R2.2 and R2.3"
- Promulgating more and more documentation that creates little value — phone number changes and you are not in compliance
- Strike business phone and address
- Senior delegation — add a line regarding what a senior manager cannot sign off on? More definition to what can be by saying what can not.
- Must say "or delegate" or it cannot be delegated
- But that implies confusion — must clarify that can only be delegated where specified
- R2.1 – single manager per entity?
- Instead add "single" up in R2 and can strike R2.1? But retain the language from the directive by moving up into R2 itself
- Replace "in adherence with" with "ongoing compliance with"
- Change to make previous changes in compliance with striking R2.1 — scriveners correction

R5.3

- Punt this one for now
- Also need to add definition for "escort"

CIP- 003 Wednesday Morning Rank, Review and Refinement

Poll on CIP 003	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=	**19**	**3**	**1**	**0**

Team and Participant Comments after the first Ranking

R2 changes

- R2.3 - provides audit trail for delegation by senior manager

- In this document might take out quotes to "senior" manager — universal edit
- This is set to deal with typical response of policy — not response to requirements
- Will deal with when take up the whole body
- Auditor can only look at and audit the policy
- Why have measures?
- Instructor training for auditors to audit to the standard, not to the policy unless the standard says to audit to the policy
- Discussion in 706 about where policy says something beyond the standard — an entry in the SAR
- Quotes around "senior" have a purpose? Put in glossary? If not capitalized then glossary does not apply
- Issue beyond standard should be in policy but does not trigger a penalty
- Look at wording single senior manager — separate responsibility between compliance and operation manager — must find single senior manager above both, who can delegate specific responsibility on particular issues
- "2"- Enough question about senior and delegation of responsibility not to put it in the first phase – difficult for large company to comply with it — prefer to pull from phase one box
- One individual signs off on certification to NERC — wrinkle is when nuclear involved and not under the same umbrella — can manage but potentially problematic
- Painting CEO into being the senior manager – but that may not be the best person
- Between a 3 and 2 — are we designing the organization? Cojoining implementation and compliance which are separate in large organizations, percolates this responsibility to the top — take direct and comprehensive language out
- Part of problem is how is the organization registered versus functional model for purposes of the standards — we have three separate entities with fiduciary vice presidents at the head of each — each entity has two separate functional entities — does that mean six filings?
- Anything commensurate with this in other sections? No
- Need to resolve issue with FERC on registered entity — suspend this and clarify then revisit
- Clarify language of legislative intent
- For many entities this will be moot at the end of the calendar year — intent of FERC is whoever is signing is prominent level and influence the positive allocation of resources to improve security of the power system
- FERC focused on "single" to be sure responsibility
- Issue is the authority to correct non-compliance and that enough resources are available to comply — person who certifies needs to be the one who can direct the resources needed to address non-compliance — that is the intent, need someone with authority to correct, not just manage
- Suggest R2 changes be removed but keep change in R2.3 and 2.1 — re-poll issue
- This assignment has to be made now
- But are we making it worse with the language in R2? Compliance has a specific meaning in the industry

- We want the guy responsible for making implementation possible — in longer term revisit the "one single" person responsible
- Minor comment — "responsibility" — we delegate authority but responsibility belongs to senior manager — replace with "authority"
- Diluting the changes despite original vote — are we letting the minority rule and water down proposals? This is not a voting tool but a way to focus discussion. Grateful that points of contention are raised — this is a good thing and is a way of strengthening the language.
- This sets up the auditability of the delegation — without the paper trail, unclear whether lower levels have authority.

2nd Poll on CIP 003 As revised	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=	**22**	**0**	**0**	**1**

Comments following 2nd Rank

- 1 Rank. The problem is that you can assign responsibility but without authority to make changes — need both words in the language
- Works for everyone else
- Check with NERC General Counsel as to the meaning of the two words and the difference between the two? Suggest members check with their counsels
- We do not have accountability assigned in this
- Heads of agencies may not be allowed to delegate accountability if it is in the law – means need to add to R2.

CIP 003 – CYBER SECURITY — SECURITY MANAGEMENT CONTROLS

CIP-003 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Security Management Controls
A2. Number: CIP-003-~~1~~2
A3. Purpose *(2nd paragraph)*
Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Leadership — The Responsible Entity shall assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
R2. 3Where allowed by Standards CIP-002 through CIP-009, the senior manager may delegate authority for specific actions to a named delegate. These delegations must be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.

R2.~~3~~ 4. The senior manager or delegate(s), shall authorize and document any exception from the

requirements of the cyber security policy.

CIP 004 – Cyber Security — Personnel & Training

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- The individuals shall be trained prior to being granted access rather than within 90 days of access
- Individuals shall be background screened prior to being granted access rather than within 30 days of access

Tuesday Comments on 1st Review of the Redline

CIP 004

- Same notes for first two

R1

- "and implement"

R2

- Lots of "ensure"s
- "carelessness"?
- some one on windows platform goes on the web for job related search — training needed to ensure they do not make mistakes
- "accidental" "unauthorized" "inadvertent" rather than "carelessness"
- more appropriate for a guidance document
- training cannot ensure but can encourage
- proper use of cyber assets includes not web surfing — already included in standards
- established who the training is for
- what was the comment that the sentence responds to?
- Move to phase two if debatable and not immediate
- Do we need to transplant everything from the FERC order into the standards?
- Depends on the wording offered by FERC — use words whenever possible, paraphrase or rephrase only as needed
- Second half of paragraph is removed and punted to next phase

R2.1.1 Emergencies

- Standard post storm procedure — puts it into the standard
- Tough on a substation but works in a center?
- Might belong in a different section , not training
- Might get questions on what constitutes and emergency
- Everything the temporary person did? That is a bit much for compliance — need alternate language — too much documentation
- Punt to phase two?
- Suggest leave in 2.1.1 and punt 2.1.2
- Change 2.1.2 to "defensive measures remain in effect"
- Move both to next phase?
- Now have no emergency provision
- Put in the parking lot the whole R2.1 section for review in phase two

R2.2

- R2.2.5-7 additional training
- Say "other security issues"
- This is where the escort training came from
- Clarification in 2.2.5 — in conflict with networking hardware?
- "security issues of electronic interconnectivity"? what does it mean?
- Three types of training — manager, real live and general awareness — maybe spell it out that simply
- 2.2.7 is a rehash and should be stricken
- But is a reply to a comment to clarify question
- Covered above
- 2.2.5 needs more work — punt to phase two — punt the whole section

R3

- Can only escort physical access not cyber access
- Okay

R3.4

- Punted under training. Moved here?
- Punt here to phase two along with R3.5 and 3.6
- What does limited escort mean? Strike "limited"

CIP- 004 Wednesday Morning Rank, Review and Refinement

1st Poll on CIP 004	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**18**	**2**	**3**	**0**

R1

- Problem and comments about granting access electronically — not the physical escorted access — we will get lots of comments
- 2 ranking- requirement to train prior to granting access — no provision for emergency process or technical exception — will not fly with industry —
- 2 ranking — must tie to R2 above — Prior to granting access?
- R2 applies to the sub parts
- Add below in R2.1 to avoid confusion
- "Prior to" is the question — lack of emergency provision or even ongoing access to trainer before access to facilities could be a problem
- Question of physical versus electronic access — also what about the GE rep who comes in to work on equipment, cannot get him agency specific training or afford to have someone stand over his shoulder full time.
- Still required to train GE representative regardless — question is whether train before or after access; that is the correction here
- Only fix is to treat emergencies as a technical exception
- Did we put language in C3 to address this situation? Put security training in with the safety training
- We have to give access electronically to technicians in Japan
- "granted such access"?

- C3 — R1.1 deals with emergency of the storm and crews coming in to work — not the maintenance from Japan
- Contractors and vendors training? Must be equivalent to what you give employees
- C3 says write policy so that emergency storm situation would not violate the standard
- If contractor is called in for maintenance or warranty, then must be trained before being allowed access
- In an emergency situation cannot put into policy
- That is already dealt with in C3 – deals with emergency
- Good example of separating out substation, control centers, etc.

2nd Poll on CIP 004	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**15**	**1**	**6**	**0**

Comments After 2nd Ranking

- Anything we can keep here and defer the controversy?
- The issue is timing of training and PRAs
- Propose a small team to try and redraft. Steve Vandenberg would like to be on the team

CIP 004 – CYBER SECURITY — PERSONNEL & TRAINING

CIP-004 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Cyber Security — Personnel & Training
A2. Number: CIP-004-~~1~~2
A3. Purpose:
Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Awareness — The Responsible Entity shall establish, maintain, and document and implement a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber security assets receive on-going reinforcement in sound security practices…
R2. Training — The Responsible Entity shall establish, maintain, and document and implement an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access. ~~within ninety calendar~~

~~days of such authorization.~~
R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program prior to ~~within thirty days of~~ such personnel being granted such access.

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Minor editorial changes only

Tuesday Comments on 1st Review of the Redline

R1.5

- Editorial
- The rest are fine
- Address specific call outs in R1.5 as needed

CIP- 005 Wednesday Morning Rank, Review and Refinement

Poll on CIP 005	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**22**	**0**	**0**	**0**

CIP 005 revisited

R1.5

- If used only for monitoring or control does it fall under this – put in "and/or" monitoring.
- Same issue under CIP 006

CIP 005 – ELECTRONIC SECURITY PERIMETER(S)

CIP-005 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Electronic Security Perimeter(s)
A2. Number: CIP-005-~~1~~2
A3. Purpose:
Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.~~Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP- 003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009. *(Staff will correct the citations)*

R2.3. The Responsible Entity shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Change RRO to RRO and also include RE.
- Several items where the word 'implement' was added to clarify that requirements must be both documented and implemented
- Item concerning the fact that dial up accessible CCA's using dial up only do not require physical security was put onto parking lot

Tuesday Comments on 1st Review of the Redline

R.1

- "The" senior manager not "a" senior manager
- "implementing"
- R1.7 — back it down to thirty days from completion of any physical system
- Same specific call outs as in CIP005
- Interpretation sce&g RFI

CIP- 006 Wednesday Morning Rank, Review and Refinement

Poll on CIP 006	*4 - Acceptable*	*3 – Minor Issues*	*2 – Only Acceptable if major issues are addressed*	*1 – Not acceptable*
Avg.=3.5	**0**	**0**	**0**	**0**

Tabled, hand off to a drafting team

Comments after Ranking

- Request for R4 — physical access include individual leaving facility — for physical access include when individual leaves as written — what is the intent?
- Only time of access not time ended or duration
- This is contentious to industry — pull until later
- "Thirty" calendar days — make it from completion of implementation, to capture the spirit and intent
- 1.4 and 1.6 need "procedures for and implementation of"
- this applies to physical facility plans
- 1.8 — must change to right numbers to match version two for consistency
- 1.7 — bad English — remove "completion of"
- Punt to a scrivener team
- prefer the original language — confuses implementation and procedures

- wordsmith starting with R1 to clean up — hand off to a team
- Interpretation of R1.1 about non-routable protocols?
- Important but recommend deferring until after FERC renders initial judgment
- Agree, but defer
- But not filed with FERC yet — will never go to FERC to act on for procedural reasons. Then handle in phase two

CIP 006 – PHYSICAL SECURITY OF CRITICAL CYBER ASSETS

CIP-006 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Physical Security of Critical Cyber Assets
A2. Number: CIP-006-~~1~~2
A3. Purpose:
Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Physical Security Plan — The Responsible Entity shall create ~~and~~ maintain and implement a physical security plan, approved by the ~~a~~ senior manager or delegate(s) that shall address, at a minimum, the following:
R1.2. Processes to identify all access points through each Physical Security Perimeter and implement measures to control entry at those access points.
R1.4. Procedures for and the implementation of the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
R1.6. Procedures for and implementation of escorted access within the physical security perimeter of personnel not authorized for unescorted access.
R1.7. Process for updating the physical security plan within ~~ninety~~ thirty calendar days of implementation of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.
R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement Standard CIP-009. *(Staff will correct the citations)*

CIP 007 SYSTEMS SECURITY MANAGEMENT

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Change RRO to RRO and also include RE.
- Removed acceptance of risk from Malicious Software Prevention (R4.1).
- Added implement under R7 Asset disposal or Redeployment.
- Editing to cite revision number
- Document maintenance was changed from review in 90 days to review documents within 30 of changes

Tuesday Comments on 1st Review of the Redline

CIP- 007

R2

- Implement

R4.1

- The use of anti-virus — document the use of and implement anti-virus
- Implement and document the use of
- Need more definition of "technical feasibility" not necessarily remove it
- What does 4.1 add that is not already in R4 — first sentence is redundant
- Return 4.1 to its original language — remove proposed edits
- Strike or an acceptance of risk from the end of the sentence

R5

- Editorial corrections

R7.1

- "sufficiently" is vague – why use it?
- Remove
- Clarify what you mean by unauthorized retrieval of data
- Punt it for now
- Look at NIST and DOD language
- Not changing approved language but parking the data storage requirements

R9

- Ninety to thirty days

CIP- 007 Wednesday Morning Rank, Review and Refinement

Poll on CIP 007	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**21**	**1**	**0**	**0**

Team and Participant Comments Following the Ranking

- Clarifications?
- What do we gain by saying establish and implement rather than document – should we be consistent
- R4.1?
- Can not just accept risk

- Explain how technical feasibility exception applies for a virus? Must have mitigating measures.
- If you have a system that can not use anti-virus software such as a substation or that would be adverse impacts if installed – best option is a network filtering anti-virus
- Is it acceptable to say there are not mitigations available if cannot use anti-virus – un-hackability is acceptable but be documented
- Is there such a thing as unhackable software?
- Developing a formal cyber security plan discussion yesterday? C6 requires a physical security plan but nothing requires a cyber security plan

CIP 007 SYSTEMS SECURITY MANAGEMENT

CIP-007 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Systems Security Management
A2. Number: CIP-007-~~1~~2
A3. Purpose:
Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R2. Ports and Services — The Responsible Entity shall establish and document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish, ~~and~~ document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches…
R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure. ~~or an acceptance of risk~~.
R7. Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ~~ninety~~ thirty calendar days of the change being completed.

CIP 008 INCIDENT RESPONSE & REPORTING

Proposed language changes include:

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Added implement when necessary to R1
- Added that testing the Cyber Security Plan does not require taking the component out of service.

Tuesday Comments on 1st Review of the Redline

CIP 008

R1

- Implement when you have an incident — when necessary
- When necessary applies grammatically to the "prepare and maintain" phrase too
- Move "implement when necessary" to the end of the sentence.

R1.4 & 1.5

- Why have requirement after action has occurred — getting approval for what you did after the fact
- You have an approved plan but realize it is not adequate and you take additional steps — now need to document that and ask if you can modify the plan
- The wording is implicit that plan has prescribed reaction to prescribe incident — depends on level of detail in a plan
- Detailed prescriptive plan that anyone after you can follow
- What are we adding here if we review plan every year?
- After action reports to revise plan for those plans that were inadequate for dealing with the plan —
- Tested your plan but cannot anticipate every possibility
- Lessons learned in 686 is different than words used here
- Punt and deal with in phase 2 for both items

R1.6

- Improving plan in response to lessons learned
- Keep "thirty days" — punt the "resulting from implementing the plan"

R1.8

- Change is good

CIP- 008 Wednesday Morning Rank, Review and Refinement

Poll on CIP 008	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptabl*
Avg.=3.5	**20**	**2**	**0**	**0**

C8

- Need to explain R1 to industry
- Better to say implement when an incident occurs – refines the word "necessary"
- In response to a Cyber Security Incident – a defined term in the NERC glossary
- Need to say suspected incident – say "potential" instead
- That creates issues – we have potential incidents all the time and do not invoke the plan – if you don't know – should be a know incident with a measurable impact
- Need to anticipate suspected or potential to invoke and update the plan as needed
- Table this for now – problem with a one level plan – defined a process to address multiple levels of plans – needs more discussion in phase two
- Someone fat fingers their password – is that an incident? Must the plan be invoked?
- Important thing is that the plan has to be implemented in response to an event – type of event does not matter – if never implemented it is because you never had an event
- Adding "potential" confuses things
- Take out "potential" – adds confusion
- Consider changing cyber security incidents by removing "a"
- Needs to be some thought or wordsmithing on a few areas – need to review suggested changes
- Any drafting need to be done before next meeting or take up in two weeks?
- Still unsettled but not sure why
- Like to revisit the whole thing in next phase
- Also concerned as to why this statement is even there

- Probably not harmful to leave in but creating an opportunity for comments that we have to respond to
- Point to industry comment and FERC order to explain why it is being addressed
- Consider second sentence: plan will be implemented in response to an cyber security incident
- Put in "implement the plan in response"
- May need to address cyber security incident definition in the next phase
- No assignment needed to address language prior to next meeting

CIP 008 INCIDENT RESPONSE & REPORTING

CIP-008 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Incident Reporting and Response Planning
A2. Number: CIP-008-~~1~~2
A3. Purpose:
Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident Response plan shall address, at a minimum…
R1.4. Process for updating the Cyber Security Incident response plan within ~~ninety~~ thirty calendar days of any changes.
R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test.

CIP 009 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Proposed language changes include

- Language to address 706 concerns to remove 'reasonable business judgment."
- Add RE in addition to RRO.
- Changes must be incorporated into the plan within 30 days of the change

Tuesday Comments on 1st Review of the Redline
CIP- 009
R1.3 & 1.4

- Similar to CIP008 – but language from the order
- Imply the action must be approved by the senior manager?

- If the document was wrong and following it would have cause problems then you need to apply the lesson, revise the plan and get it approved
- Is 1.4 a restatement of 1.3? No, first is a justification and 1.4 is revise the plan
- This does not read right
- Punt this one for redraft

R3

- "Thirty days"

CIP-009 Wednesday Morning Rank, Review, and Refinement

Poll on CIP 009	*4 — Acceptable*	*3 — Minor Issues*	*2 — Only Acceptable if major issues are addressed*	*1 — Not acceptable*
Avg.=4.0	**22**	**0**	**0**	**0**

CIP-009 DRAFT REDLINE LANGUAGE AS OF END OF MEETING, 10-8-08

A1. Title: Cyber Security — Recovery Plans for Critical Cyber Assets
A2. Number: CIP-009-~~1~~2
A3. Purpose:
Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. ~~Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment~~.
A4. Applicability:
Add: 4.1.12 Regional Entities.
A5. Effective Date: ~~June 1, 2006~~

B. Requirements
R3. Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ~~ninety~~ thirty calendar days of the change being completed.

G. TEAM BUILDING- GO LEFT- GO RIGHT PREFERENCES

The Team engaged in a brief exercise to highlight the members' individual preferences for problem solving and decision-making. *(See Appendix #7 for the results of the exercise)* Following the exercise the facilitator noted that a sign of a well balanced group includes a diversity of work styles. For example having some who prefer to pay attention to task and others who prefer to pay attention to people issues can be very helpful. These are not either/or preferences but signal for the Team how they individually and collectively come at the issues. Finally they can help group leaders and those assisting in process by, for example, noting a distinct preference for morning and trying not to take on the hardest issues late in the afternoon.

H. REVIEW OF PHASE I MEETING SCHEDULE AND DRAFTING ASSIGNMENTS

1. In Person Meetings and WebEx Schedule

Session Type	Dates	Agenda
Webex/Conf call session	Oct 15	Individual sub team Webex's to review their respective Phase I assignment deliverables in advance of full team review during October 21-22 meeting in Sacramento.
In person meeting at SMUD (Sacramento, Kevin Sherlin)	October 21-22 Full/Full	Review and comment upon sub team straw proposals.
Webex/Conf call session	Oct 29	Finalize the Phase I posting documents and submit to MEL
WebEx/conf call session	Nov 5 - NERC staff feedback	Review and conform drafts per feedback from MEL
In person meeting at Princeton, NJ (confirmed)	Nov 12-14 Half/Full/Half	Phase II
WebEx/conf call session	Nov 18 Webex/Conf call	Phase II
In person meeting at FERC offices or Charlotte	December 4-5 Full/Full	Phase II
In person meeting at APS (Phoenix, Bill Winters) or BPA (Portland WA, Jon Stanford)	January 7-9 Half/Full/Half	Consider Comments to Phase I posting

2. Assignments

	Task	Leader	Sub team	Due Date
1	CIP-004 R2 and R3	Jackie Collett	Chris Peters, John Varnell, Sharon Edwards	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
2	CIP-006 R1	Kevin Perry	Joe Doetzl, Scott Fixmer, Thomas Hofstetter	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
3	Review Measures	Jerry Freese	Keith Stouffer,	Straw Proposal due to

	associated with changes in CIP-002 to CIP-009		Roger Lampila, Todd Thompson	sub team leader on October 14 in advance of sub team WebEx on October 15
4	Implementation Plan – update to address newly identified CA	Scott Mix	Michael Winters, Dave Norton, Kevin Perry	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
5	Implementation Plan update to address revised Requirements from Phase I and Mapping document – matrix that compares current version of standard with revised version with a comment that explains what changed.	Phil Huff	Kevin Sherlin, Scott Rosenberger, Jon Stanford, Scott Mix	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
6	Comment Form – including an extensive write-up of the background, rationale for revisions, explanatory text.	Jeri Domingo-Brewer	Steve Vandenberg, Harry Tom, Sharon Edwards, John Lim	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15
7	Review VRFs associated with changes in CIP-002 to CIP-009	Todd Thompson	Roger Lampila	Straw Proposal due to sub team leader on October 14 in advance of sub team WebEx on October 15

I. AFTER-ACTION REVIEW AND EVALUATION

At the conclusion of the meeting, the Team offered an evaluation of the process including what worked and what could be improved. *(See Appendix # 4 for the Team's review and suggestions.)*

Adjourned at noon on Wednesday October 8, 2008.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1

SDT Cyber Security Order 706 1st Meeting Agenda

October 6, 2008 — 1 PM to 5 PM EST
October 7, 2008 — 8 AM to 5 PM EST
October 8, 2008 — 8 AM to 12 Noon EST

National Institute of Standards & Technology
100 Bureau Drive
Gaithersburg, MD

WebEx Password: standards	Conf Call dial-in number (732) 694-2061
WebEx Meeting numbers: Monday 711 925 616 Tuesday 713 677 232 Wednesday 712 239 082	Conference Codes: Monday 12081006082 Tuesday 12081007081 Wednesday 12081008082

Monday October 6, 2008

1. Opening remarks — Michael Assante, CSO, NERC
2. Review NERC Antitrust Compliance Guidelines — Harry Tom
3. Welcome and Introductions — Jeri Domingo-Brewer/Kevin Perry
4. Overview of NERC Standards Development Process — Gerry Adamski/Dave Taylor
5. Review of CSO706 SAR — Dave Norton

Tuesday October 7, 2008

6. Overview of NIST Risk Management Framework — Keith Stouffer
7. Comparison of NIST and NERC Cyber Standards — Keith Stouffer
8. Project Roadmap – Jeri Domingo-Brewer with facilitation assistance

Wednesday October 8, 2008

9. Project Roadmap Wrap-up (facilitated)
10. Next Steps
11. Plan future meetings schedule

Appendix # 2

Cyber Security for Order 706 Standard Drafting Team and Attendees List
Project 2008-06 — CSO 706 SDT

D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
Jeri Domingo Brewer, Chair	U.S. Bureau of Reclamation
Jackie Collett	Manitoba Hydro
Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
Joe Doetzl	Manager, Information Security. Kansas City Power & Light Co
Sharon Edwards	Project Manager, Duke Energy
Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corporation
Gerald S. Freese	Director, Enterprise Information Security American Electric Power
Tom Hofstetter	Midwest ISO, Inc.
Philip Huff	Arkansas Electric Cooperative Corporation
John Lim,	CISSP, Department Manager, Consolidated Edison Co. of New York
David L. Norton	Policy Consultant - CIP Entergy Corporation
Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
Christopher A. Peters	ICF International
David S. Revill	Georgia Transmission Corporation
Scott Rosenberger	Luminant Energy
Kevin Sherlin	Sacramento Municipal Utility District
Bryan Singer	Wurldtech Security Technologies
Jon Stanford	Bonneville Power Administration
Keith Stouffer	National Institute of Standards & Technology
Steve Vandenberg	BC Hydro Power Supply
John D. Varnell	Technology Director, Tenaska Power Services Co.
Michael Winters	Arizona Public Service Co.
William Winters	Hydro One Networks, Inc.
Roger Lampila	*NERC Regional Compliance Program Coordinator*
Scott Mix	*NERC Manager of Situation Awareness and Infrastructure Security,*
Todd Thompson	*NERC Regional Compliance Program Coordinator*
Harry Tom	*NERC Standards Development Coordinator*
Bob Jones, Stuart Langton, Hal Beardall	*Facilitators, FSU/ FCRC Consensus Solutions Center*

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

List of Attendees — Cyber Security Order 706

Standard Drafting Team Meeting
National Institute of Standards & Technology — Gaithersburg, MD
October 6–8, 2008

Attending in Person- Team Members

1. D. Jack Bernhardsen	President/Manager Pacific Northwest Security Coordinator, Inc.
2. Jeri Domingo Brewer, Chair	U.S. Bureau of Reclamation
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
5. Joe Doetzl	Manager, Information Security. Kansas City Power & Light Co
6. Sharon Edwards	Project Manager, Duke Energy
7. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corporation
8. Gerald S. Freese	Director, Enterprise Information Security American Electric Power
9. Tom Hofstetter	Midwest ISO, Inc.
10. Philip Huff	Arkansas Electric Cooperative Corporation
11. John Lim,	CISSP, Department Manager, Consolidated Edison Co. of New York
12. David L. Norton	Policy Consultant - CIPEntergy Corporation
13. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
14. Christopher A. Peters	ICF International
15. David S. Revill	Georgia Transmission Corporation
16. Scott Rosenberger	Luminant Energy
17. Kevin Sherlin	Sacramento Municipal Utility District
18. Jon Stanford	Bonneville Power Administration
19. Keith Stouffer	National Institute of Standards & Technology
20. John D. Varnell	Technology Director, Tenaska Power Services Co.
21. Michael Winters	Arizona Public Service Co.
22. William Winters	Hydro One Networks, Inc.
1. David Taylor	*NERC*
2. Harry Tom	*NERC*
3. Michael Assante	*NERC*
4. Roger Lampila	*NERC*
5. Scott R Mix	*NERC*
6. Todd Thompson	*NERC*
7. Gerry Adamski	*NERC*
8. Robert Jones	*FSU/FCRC Consensus Solutions Center*
9. Stuart Langton	*FSU/FCRC Consensus Solutions Center*
10. Hal Beardall	*FSU/FCRC Consensus Solutions Center*

SDT Team Member Attending via Webex *(in order of roll call, October 6)*

1. Steve Vandenberg	BC Hydro

SDT Members Unable to Attend or Participate by Webex

1. Bryan L. Singer*	Kenexis

Attending in Person- Participants

	NAME	COMPANY
1	Marshall Abrams	MITRE
2	Markus Braendle	ABB
3	James Brenton	ERCOT

4	Jerome Farquharson	Burns & McDonnell Engineering
5	Roger Fradenburgh	Network & Security Technologies
6	Stu Katzke	NIST
7	John Joseph McGlynn IV	PJM
8	Steve McElwee	PJM Interconnection
9	Dan Mishra	Midwest ISO
10	Peter Nelson	Network & Security Technologies
11	Mike Peters	FERC *(October 6 & 7 in person, October 8 by phone)*
12	Mark Simon	Encari
13	Michael Toecker	Burns & McDonnell Engineering

Attending via Webex- Participants *(in order of roll call, October 6)*

2	Mike Mertz	Southern California Edison
4	Alex Tatistcheff	Idaho Power
5	Regis Binder	FERC
6	Mike Fischette	Lansing Board of Water and Light
7	Phil Sobol	Corporate Risk Solutions, Inc
8	David Dunn	IESO
9	Dan Thanos	GE
10	Vicki O'Leary	NGRID
11	Boyd Nation	Southern Company
12	Dave Batz	Alliant Energy
13	John Friday	Reliant Energy
14	Rodney O'Brian	Southern Company
15	Steve Brezina	WAPA
16	Matt Schnell	Nebraska Public Power District
17	Karen Yoder	First Energy
18	Mike Puscas	United Illuminating
19	Doug Johnson	Commonwealth Edison
20	Chip Lees	
21	Ameren — Hoang Ngo	Reliant
22	James Bassett	IPC

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

Participants in NERC activities (including those of its committees and 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 participants' marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and

subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

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

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

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

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

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

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

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

Appendix # 4
After Action Review and Team Process Evaluation

What did you think was most effective about the meeting?

- This is a high performance group with experience and openness to listen and work together through disagreements — everyone participated
- Meeting preparation — Scott 's Phase 1"strawman" was something we could discuss and that was key. Information Harry sent in advance was very helpful
- Members and participants offered constructive solutions that we could rally around
- Helped to have someone else to push us through (i.e. facilitate) allowing the chair and vice chair to more fully participate without having to worry or focus on process
- First time with an outside facilitator for some members- very much helped
- Having senior NERC staff on hand (Gerry, David, Harry, Scott) saved lots of time and helped Team understand how this works.
- Sharon's note taking was well done, very helpful and will help the facilitators produce an accurate summary and record of the sessions
- Thank NIST for all their hard work — their review will benefit us as we move forward into Phase 2.
- Harry responding to everyone's requests was very helpful
- Thank you to the facilitators — positive experience to share with other drafting teams
- Thanks to Keith for hosting and all of his work behind the scenes to pulling this meeting off

Suggestions for next meeting – Should we do anything differently?

- Larger room would have helped
- Need more microphones for those on the phone to hear what those in the room are saying — need to assure quality of system too. This is an important investment in those participating beyond the team members.
- Internet access during the meeting to pull up documents as needed — and power strips for computers.
- Computer running projection should be separate from the WebEx computer — one running WebEx and a second to access research m whatever is running the projector should be separate from meeting host — allows you to use raise hand tool on WebEx

Other suggestions:

- Table purpose statement and any other organizational issues (consensus procedures, roles, etc.) until next full meeting

- Team meeting presentation materials will be posted on the NERC Team webpage. They will be referenced in the meeting summary as appendices and links. They will be clearly labeled as presentation and informational briefing materials for the Team's consideration, not Team products. This will also be made clear in the meeting summary.

Appendix #5
Standard Authorization Request (SAR)
Revisions to Critical Infrastructure Protection Standards (revisions to CIP-002 through CIP-009, June 9, 2008))

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

Appendix #5
CIP 002-009 Redline Straw Man Draft, October 8, 2008
CIP 002-009 Clean Straw Man Draft, October 8, 2008

Click on the following link for the document:

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

Appendix # 6 SDT Draft Consensus Guidelines

DRAFT CONSENSUS GUIDELINES

CONSENSUS DEFINED

Consensus is a **process**, **an attitude and an outcome**. Consensus processes can produce better quality more informed products.

A. Consensus is a problem solving process in which all members:

1. Jointly distinguish their concerns
2. Educate each other
3. Jointly develop alternatives and then
4. Adopt recommendations everyone can embrace or at least live with.

In a consensus process, members can honestly say:

- I believe that other members understand my point of view
- I believe I understand other members' points of view
- Whether or not I prefer this decision, I support it because it was arrived at openly and fairly and because it is the best solution for us at this time

B. Consensus as an attitude provides that each member commits to work toward agreements that meet their own and other member needs and that all can support the outcome.

C. Consensus as an outcome means that agreement is reached by all members or by a significant majority of members. The level of enthusiasm for the agreement may not be the same among all members on any issue, but on balance all should be able to live with the overall package. **Levels of consensus** can include:

- Participants strongly support the solution
- Participants can "live with" the solution
- Some participants do not support the solution but agree not to veto it.

DRAFT CONSENSUS GUIDELINES

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards including assessment of the reliability and market interface impacts.

General consensus is a participatory process whereby, on matters of substance, the members strive for agreements which all of the members can accept, support, live with or agree not to oppose. In instances where, after vigorously exploring possible ways to enhance the members' support for the final package of recommended revisions, and the Team finds that 100% acceptance or support is not achievable, final consensus recommendations will require at least 75% favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the Team finds that even 80% acceptance or support is not achievable, the Team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50% support from the Team.

The Team will develop its recommendations using consensus-building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The Team's consensus process will be conducted as a facilitated consensus-building process. Team members, NERC staff and facilitators will be the only participants seated at the table. Only Team members may participate in discussions and vote on proposals and recommendations. The Chair and Vice Chair may request specific clarification from observers in order to assist the Team in understanding an issue. Observers/members of the public are welcome to speak during a public comment period that will be provided at each meeting, and all written comments submitted on the comment forms will be included in the Team and facilitators' summary reports.

To enhance the possibility of constructive discussions as members educate themselves on the issues and engage in consensus-building, members agree to refrain from public statements that may prejudge the outcome of the Team's consensus process. In discussing the Team process with the media, members agree to be careful to present only their own views and not the views or statements of other participants and/or may direct such inquiries to the Team Chair and Vice Chair. In addition, in order to provide balance to the Team process, members agree to represent and consult with their stakeholder interest group.

MEETING GUIDELINES FOR PARTICIPANTS

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")

- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

CONSENSUS BUILDING TECHNIQUES

- **Brainstorming.** (green light thinking — not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions.** This helps the facilitator determine the speaking order. Team and participants will raise name tent to speak. Facilitator(s) will call on participants in turn. The Facilitator(s) may interrupt the stack (change the speaking order) in order to promote discussion on a specific issue or, to balance participation and allow those who have not spoken on a issue an opportunity to do so before others on the list who have already spoken on the issue.

- **"Parking Lot" —** a list of issues that are raised but set aside to be addressed at a later time in the meeting or subsequent meeting.

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.
  - Use to guide and focus discussion, not used as a voting mechanism. Rather it is a poll to see where folks are.
  - Must be prepared to offer refinements and suggestions to address serious concerns.

  4 = Proposal is acceptable as it is
  3 = Proposal is acceptable; I can live with it but there are minor concerns to address
  2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
  1 = Proposal is not acceptable

Appendix #7
Team Building- Go-Left/Go Right Exercise Results

"Go Left/Go Right"
Work Style Preferences

Team Members absent: Jay S. Cribb, Bryan Singer and William Winters

Detail Oriented	Big Picture Oriented
Jackie Collett, Tom Hofstetter, Kevin B. Perry, Scott Rosenberger, Kevin Sherlin, Keith Stouffer	Jack Bernhardsen, Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, David S. Revill, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters

People Focus	Task Focus
Jack Bernhardsen, Jackie Collett, Joe Doetzl, Sharon Edwards, Tom Hofstetter, Christopher A. Peters, Jon Stanford, Steve Vandenberg	Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, Kevin B. Perry, David S. Revill, Scott Rosenberger, Keith Stouffer, Michael Winters

Middle: John D. Varnell,

Facts and Information	Intuition, Gut Feelings
Jack Bernhardsen, Jackie Collett Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Scott Fixmer, Tom Hofstetter, David Norton, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg	Sharon Edwards, Gerald S. Freese, Christopher A. Peters, Jon Stanford, Michael Winters

Middle: John D. Varnell,

Spontaneous, Flexible	Structured, Organized
Jack Bernhardsen, Gerald S. Freese, Philip Huff, John Lim, David L. Norton, Christopher A. Peters, John D. Varnell	Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Kevin B. Perry, David S. Revill, Scott Rosenberger, Kevin Sherlin, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Outgoing, Talkative	Reserved, Reflective
Jackie Collett, Gerald S. Freese, David Norton, Kevin B. Perry, Kevin Sherlin, John D. Varnell	Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Philip Huff, Christopher A. Peters, David S. Revill, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Middle: Scott Rosenberger

Tactical, Short Term	Strategic, Long Range
	Jack Bernhardsen, Jeri Domingo Brewer, , Joe Doetzl, Sharon Edwards, Scott Fixmer, Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Christopher A. Peters, David S. Revill, Kevin Sherlin, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters

Middle: Gerald S. Freese

Rule with Head	Rule with Heart
All	None

Afternoon Person	Morning Person
Jack Bernhardsen, David Norton, Christopher A. Peters, Kevin Sherlin, David S. Revill	Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters

Sprit of the Law	Letter of the Law
Jack Bernhardsen, Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese Tom Hofstetter, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Jon Stanford, Steve Vandenberg, Michael Winters	Jackie Collett, Scott Rosenberger, Kevin Sherlin, David S. Revill

Middle: John D. Varnell

Team Player	Individual Achiever
Jack Bernhardsen, Jeri Domingo Brewer, Joe Doetzl, Sharon Edwards, Scott Fixmer Tom Hofstetter, Philip Huff, David Norton, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Kevin Sherlin Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jackie Collett, Gerald S. Freese, John Lim, Scott Rosenberger

Focus on Results	Focus on Process
Jeri Domingo Brewer, Jackie Collett, Joe Doetzl, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Tom Hofstetter, Philip Huff, David Norton, Keith Stouffer, Kevin Sherlin, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jack Bernhardsen, John Lim, Kevin B. Perry, Scott Rosenberger,

Doer	Planner
Jack Bernhardsen, Jackie Collett, Sharon Edwards, Gerald S. Freese, John Lim, Kevin B. Perry, Scott Rosenberger, Keith Stouffer, Kevin Sherlin John D. Varnell, Michael Winters	Jeri Domingo Brewer, Joe Doetzl, Scott Fixmer, Tom Hofstetter, Philip Huff, David Norton, Jon Stanford, Steve Vandenberg

Confront Issues Directly	Handle Issues Indirectly
Jack Bernhardsen, Jackie Collett, Sharon Edwards, Scott Fixmer, Gerald S. Freese, Philip Huff, John Lim, David Norton, Kevin B. Perry, Scott Rosenberger, Jon Stanford, Steve Vandenberg, John D. Varnell, Michael Winters	Jeri Domingo Brewer, Joe Doetzl, Tom Hofstetter Keith Stouffer