NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

October 21, 2008 | 8 a.m.–5 p.m.
October 22, 2008 | 8 a.m.–noon
Sacramento Municipal Utility District
Sacramento, CA

MEETING SUMMARY CONTENTS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendices

Meeting Facilitation and Draft Report By: Stuart Langton & Hal Beardall
FCRC Consensus Solutions — Florida Conflict Resolution Consortium**, Florida State University**
Thanks to Team members Sharon Edwards and Kevin Perry, and NERC Staff Harry Tom for their meeting notes.
http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html

EXECUTIVE SUMMARY

A. Introductions, Agenda Review, and Welcoming Remarks

The Chair, and Vice Chair welcomed the members and reviewed with the team and participants the proposed meeting agenda *(See appendix #1*). NERC staff Harry Tom conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then and thanked Kevin Sherlin for hosting the meeting at the Sacramento Municipal Utility District offices.

B. Review of NERC Antitrust Compliance Guidelines

Harry Tom 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 the guidelines as they would cover all participants and observers.

C. Acceptance of Organizational Meeting Minutes

Stu Langton and Hal Beardall, with the FCRC Consensus Solutions facilitation team, reviewed the minutes from the first meeting noting corrections. The group agreed to accept the minutes as they were distributed to the group with the minor corrections noted; however the minutes will be open to additions as necessary.

D. Planning Challenges, Purpose Statement, and Consensus Guidelines

Stu Langton provided an overview of organizational issues and planning challenges the drafting team will need to keep in mind such as organization, process, issue identification, progression strategy and schedule.

Mr. Langton suggested some key principles for the group such as the capacity to tolerate ambiguity and patience. This will be an iterative process that will build on previous discussions while flexible enough for the group to revisit earlier issues if needed as a result of subsequent discussions.

Following the challenges and principles, Mr. Langton offered for the group's consideration the following draft purpose statement as a starting point for review and discussion:

> "The overall purpose of the Cyber Security of Order 706 SDT is to work together to build consensus on a package of recommended draft cyber security standards and implementation plan that is responsive to and consistent with the scope of the SAR and the FERC Order 706.
>
> The team's products will seek *to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system* and will be submitted for consideration by the registered ballot body. *(Italics from the SAR "purpose" statement)"*

Following discussion and suggestions for improvement, the group asked the facilitators work with the chair and staff to reframe the scope based on this discussion and bring a new draft back to the full group for review next time

Mr. Langton provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6).* He noted that consensus could be understood as having three meanings in a group process: it is an attitude, an outcome or decision rule, and 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 suggested that the team review this again at the next meeting with an eye towards adopting a procedure going forward.

Mr. Beardall reviewed a set of ground rules *(See, Appendix #6)* for the meeting including additional items added at the first meeting for phone protocols.

E. Reviewing Sub-team Draft of NERC CIP Standard

Mr. Langton reviewed the drafting sub team assignments (*Appendix #4*). Sub team leader Jackie Collett described the revisions offered for consideration by the CIP 004 sub team. *(See appendix #5 for link to red-line/underline revisions)*

Sub team changes included:

- Improved the wording
- Took out reasonable business judgment
- Training to be completed prior to granting access
- Personnel risk assessment to be completed prior to granting access
- Added provision that emergency provisions should be handled in accordance with CIP 003.R.1.1.

Following team comments regarding proposed changes to CIP 004 the group voted on the following three options for references to emergencies concerning Training and Background Screening Pre-Requisites:

A. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access. (No reference to emergency provisions.)
B. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. (Note: This option includes language included in FERC 706 language specifically.)
C. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. Emergency provisions should be handled in accordance with CIP 003.R1.1. (Note: This option includes reference back to CIP 003 Policy within CIP 004 R.2&3 to deal with Emergency situations.)

Vote on accepting the proposed CIP 004 language

Preferences	Option A Above	Option B Above	Option C Above
Voting Members	0	22	2

The facilitators suggested an initial acceptability rating (using the 4-3-2-1 scale) of the preferred option to guide additional discussion and refinement.

Acceptance of CIP 004 Proposed Changes	4	3	2	1
Voting Members and Observers	16	8	2	0

Following team discussion and suggestions the group came to the following conclusions concerning CIP 004:

- CIP 004 was accepted with the changes to require the Cyber Security training and background screening prior to access and with the inclusion of language concerning emergency provisions in accordance with FERC Order 706 (Option B above).
- CIP 003 Policy language will be reviewed/modified by a work group in Phase II, not Phase I.

F. Technical Feasibility Exception proposal

Michael Assante, NERC Chief Security Officer, addressed the group by phone and asked the team to consider addressing the technical feasibility exception as a priority and possibly as part of Phase I. Mr. Assante pointed to the request from FERC to address this issue and reviewed several of the related issues to be considered.

Following team discussion of the request the Chair offered a motion to table the issue of the Technical Feasibility Exception until after the team agenda is completed. Members voted unanimously in favor of the motion with one abstention.

G. Reviewing Sub team draft of NERC CIP Standard 006

Kevin Perry, as CIP 006 sub team leader, provided an overview of the revisions offered by the sub team in CIP 006 for consideration by the full team: *(See appendix #5 for link to red-line/underline revisions)*

- Removed Reasonable Business judgment;
- Changed dates as appropriate;
- Minor wording changes which did not alter the substance of the requirement
- R1.6 added that procedures for the active monitoring of escorted persons at all times are required;
- R1.8 added that the Physical Security Plan must be reviewed annually;
- R2. (Note: The prior 1.8 requirement becomes R2 in this proposal. The original suggested language follows:

- R2. Protection of Physical Access Control Systems — Cyber Assets authorizing and logging access to the Physical Security Perimeter(s) shall:
    - R2.1. Exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall reside within an identified Physical Security Perimeter or be physically monitored 24x7 by personnel authorized unescorted access.
    - R2.2. Be afforded the protective measures specified in Standard CIP-003-1; Standard CIP-004-1 Requirement R3; Standard CIP-005-1 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-1; Standard CIP-008-1; and Standard CIP-009-1.

After an initial team discussion and questions for clarification, the team offered the following initial acceptability rating:

Acceptance of CIP 006 Proposed Changes	4	3	2	1
Voting Members	10	7	2	0

As a result of team discussion of the initial acceptability ratings the following revised CIP 006 language was proposed and tested for acceptability:

- R2. Protection of Physical Access Control systems – Cyber Assets that authorize and/or log access to the Physical Security Perimeters(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic mechanisms and badge readers, shall:
- R2.1 be protected from unauthorized physical access
- R2.2 be afforded the protective measures specified in Standard CIP 003-1; Standard CIP 004-1 Requirement 3; Standard CIP 005-1 Requirements R2 and R3; standard CIP 006-2 Requirement R4 and R5; Standard CIP 007-1; standard CIP 008-1; and Standard CIP 009-1.

Acceptability Rating for CIP 006 with Revised Proposed Language:

Acceptance of CIP 006 Proposed Changes	4	3	2	1
Voting Members	15	8	0	0

H. Review of Sub Team Report on Measures & VRFs

Jerry Freese, leader for the sub team on measures, reported that their team performed a review of the measures, but based on changes prior to today's meeting; they believe there are no changes to the measures in response to proposed changes in CIP requirements.

Todd Thompson reported on behalf of the sub team reviewing VRFs that they believe no changes need to be made at this time.

I. New Implementation Plan for Changes to the Existing Requirements after Phase I Changes

Phillip Huff reported on the progress with the Implementation plan for new or changed Phase I requirements and the accompanying table including the following proposed language: *(See appendix #5 for link to red-line/underline revisions)*

- Proposed language: the original proposed effective date discussed for the modifications contained in these standards is the greater of (1) 180 days following approval by the FERC or (2) the number of days following approval by FERC before a Responsible Entity must become Compliant with a requirement according to the associated Compliance Schedule.

Based on team discussion, the sub team will make additional edits for consistency with changes made in the body of the document and make conforming changes to the standards as identified in review for creating the table.

J. COMMENT FORM REVIEW

Chairman Jeri Domingo-Brewer reviewed the sub team progress on the comment form: *(See appendix #5 for link to red-line/underline revisions)*

- Background information Section uses language out of the SAR to explain what the team had agreed to
- Summary of Phase I Revisions Section summarizes each of the changes
- Requests for Comments/Questions Section requests feedback from commenters

During discussion the team noted that CIP-004, CIP-006 and the Implementation Plan changes need to be updated in the Comment Form. The team also noted the need for education to the industry through a robust communication plan. The team accepted that this draft as a good start on the Comment form.

Members agreed to adjourn for the day.

A. Day Two — Welcome and Agenda Review

Chairperson Jeri Domingo-Brewer thanked the members of the sub teams for their hard work and reviewed the progress made by the group yesterday. She stated that today the team would:

- Review work from the remaining sub teams that were not reviewed yesterday;
- Hanging issue that the group needs to consider pertaining to CIP 006;
- Consider the issue of Technical Feasibility based on the request yesterday from Mike Assante of NERC asking the group to add this issue to the agenda for this meeting.

Stu Langton, with the FCRC Consensus Solutions facilitation team, noted the broad range of expertise members brought to the table and the need to build a common understanding of issues. He asked individuals who raise questions or concerns to also offer a proposed solution or alternatives to help the group move forward.

B. Implementation Plan Amendments

Scott Mix, sub team lead, reviewed the work that has been done so far concerning implementation plans for new assets and other situations that will be covered under CIP standards in the future. The work included a summary, a narrative explanation of each category, and a timetable. *(See appendix #5 for link to red-line/underline revisions)*

He reviewed who and when an entity would need to be compliant. He noted three milestone categories:

- **Category 1** entities starting from scratch. Existing Table 4 will be used.
  - ***The first identified Critical cyber Asset for a Registered Entity***
  - 24 months to become compliant and 36 months to become auditable compliant.
- **Category 2** is for an entity that already has a schedule and is doing things but they have identified a newly identified Critical Asset.
  - ***Reclassification or change in status of an existing Critical Asset to a Critical Cyber asset.***
  - Questions were raised concerning how the proposed tables would work when/if the CIP standards apply to nuclear. There was no answer provided at this time, as there are many variables which still need to be resolved.
  - Mergers
    - For mergers and acquisitions there is a one-year period to bring the two programs of the different companies into harmony.
    - After that one year and after completing the original CIP compliance tables, they would need to comply with the proposed category 2 timetable.

- **Category 3** deals with new assets within an existing Critical Asset. The assumption is that because you are doing something active and that you do not turn on the asset until you have completed the compliance needs within the construction.
    - ***An existing Critical Asset Replacement, reconfiguration, upgrade, or addition of a relevant cyber Asset associated with an existing Critical Asset.***
    - Construction of an asset (substation, etc.) that will be declared Critical upon activation
    - Replacement or upgrade of a Critical Asset
    - Addition of a Critical Cyber Asset at an existing Critical Asset

Scott Mix reviewed the various time thresholds which the sub team is proposing for compliance with the various situations described in the above categories.

As part of the team discussion the Vice Chair offered 6 different scenarios and how each type of scenario could be gamed by entities to gain time for compliance. The Chair asked team members to submit suggested treatments of example scenarios that summarize the categories. The suggestions should ask 3 questions and categorize appropriate events. The sub team will review suggestion during the WebEx on October 29. The Chair also asked that the team to review the comment form and provide related input to the Comment Form Sub Team.

C. CIP 006 Un-resolved Issue

An additional proposed modification to CIP 006 R1.6 language was discussed and accepted by the group as follows:

- Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

D. CIP 003 Changes and Discussion

Proposed changes were offered to CIP 003 as follows: *(See appendix #5 for link to red-line/underline revisions)*

CIP 003 R2: Leadership — The Responsible Entity shall assign a single 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.

a. NERC audit compliance staff clarified that the Responsible Entity may be either the Corporation as a whole or may be the Registered Entity functions (GO, TO, BA, etc.).
b. **CIP 003 R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. ~~taken or a statement accepting risk. and/or any residual risk~~

After reviewing several suggested changes, members were asked to rate the language as revised above striking "or acceptance of risk":

The SDT's first initial rating on acceptance of the proposal:

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
Voting on the above by SDT	11	7	1	0

Following additional discussion, members were asked to rate the proposal again without the word "any" before "compensating measures":

The SDT's second vote on acceptance of proposed language change:

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
Voting on the above by SDT	12	6	4	0

Following additional discussion, members agreed to retain the word "any".

There was general agreement around the room that in CIP 007 wherever the phrase "acceptance of risk" appears, it will be removed even though each such instance where the phase appears may not have been discussed at length.

E. Proposal to Substitute "Prudent Judgment" for "Reasonable Business Judgment"

Member John Varnell requested the group consider substituting the term "prudent judgment" in place of the term "reasonable business judgment." Due to a lack of support, the group decided not to move forward with the replacement of the term "reasonable business judgment" with 'prudent judgment."

F. Proposed a Definition of Access Control System

As requested by the drafting team, Scott Mix offered a draft definition of Access Control System as follows:

> A system which provides for Authorization, Authentication, and frequently Accounting of access through either a Physical Security Perimeter or an Electric Security Perimeter. An Access Control System may be a single computer system

which performs all three functions or may be a combination of two or more computer sub systems which work together to accomplish all three functions.

i. Authentication is the process of verifying a users or object's identify.
ii. Authorization is process for granting an authenticated user or object's the authority to perform a certain operation.
iii. Accounting provides an audit trail of access, and includes logging of access by identification and time.

The SDT was asked to submit their comments for the resolution of preferences concerning the definition to Vice Chair, Kevin Perry.

G. Technical Feasibility

The Chair noted that there were two potential proposals (one from Scott Mix and one from Keith Stouffer) for addressing "technical feasibility" exception in Phase 1. She asked the team to listen to each of the proposals, consider the proposals, and decides if one of the alternatives offered could be included within the Phase I work of this team.

Scott Mix reviewed material directed in the FERC Order 706. He noted that FERC wants a framework includes mitigation steps, regular review, justification, internal approval by the senior manager, wide area approval through the ERO audit process, and cooperation with the ERO to provide the Commission with high level impact of the technical feasibility on the reliability of the grid.

Keith Stouffer of NIST provided an alternative proposal on Technical Feasibility noting it is addressed within the NIST framework for risk management and describing what a responsible entity shall document for all Technical Feasibility exceptions in an Exception Plan.

Scott Mix also reviewed the current Self Reporting Process. Based on the similarities between FERC directives and the items required by a self-reporting of non-compliance, Scott suggested that this same process be used for Technical Feasibility Exceptions.

Scott Mix reviewed similarities between the proposals:

Keith Proposal	Scott Proposal
A justification why the Technical Feasibility exception is necessary	Document non compliance to a specific requirement c. Provide explanation d. Describe reliability impact e. Describe any external or extraneous factors
Compensating controls or mitigation steps that provide a comparable level of security	
A plan of action, milestones, and schedule for	Provide mitigation schedule

implementing the compensating controls.	Provide mitigation plan
Obtain approval by the senior manager	Obtain Senior Officer signature
	Catalog and approval by Regional Entity
ERO must annually audit compliance with the Exception plan	Catalog and approval by ERO May trigger accelerated audit schedule Annual review and re-approval by Responsible Entity and ERO
ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System	ERO to develop separate annual report to FERC Analyze the combined impact of all Technical Feasibility exemptions
	Report will contain sensitive information — must be CEI protected
	Submit to FERC (US Entities)

As a result of team discussion the following proposal was suggested and tested:

Proposal Prepare a 'conceptual' document to seek stakeholder consideration and feedback that describes a Technical Feasibility Exception process that parallels existing compliance self report process.

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable
1st Poll — Voting SDT	20	2	0	0

As a next step for it was agreed that a sub team of Tom Hofstetter, John Varnell, Keith Stouffer, Scott Mix, Jerry Freese and possibly someone from NERC compliance, would draft a document described above for presentation at the next full team meeting.

H. Assignments and Next Steps for the Next Meeting

The team and staff reviewed the deadlines for revised drafts for review at the WebEx, October 29. In addition the team reviewed the schedule of meetings and possible topics over the next three months as follows:

- WebEx, November 3 — develop concept document for Technical Feasibility. Deliver to full team by November 7 or 10.
- WebEx, November 5 — following NERC Staff feedback, review and conform drafts per feedback.
- November 12–14 — full team meeting in Little Rock, Arkansas to finalize Phase I documents as needed and review proposed roadmap
- December 4 or 5 — In person meeting at FERC Offices in Washington, DC
- January 7–9 — In person meeting at APS in Phoenix, AZ

The Chair suggested that in December the group may begin to hash out the large issues still to be addressed. The Vice Chair offered two alternatives to the "Roadmap" going forward, a multiple phase or single phase approach and proposed the SDT use an incremental approach.

The FCRC Consensus Solutions facilitation team were asked to develop a one page proposal (big picture straw proposal and guiding principles) for addressing the remaining issues following Phase I for review and discussion by the full group at the next meeting in Little Rock, Arkansas. Member discussion today has included several key principles that could guide development and discussion of remaining issues.

The team quickly reviewed the remaining list of "Parking Lot" issues identified at the first SDT 706 meeting in Gaithersburg and not already addressed today.

I. What Did and Did Not Work Well

At the conclusion of the meeting, the facilitators asked the team to offer an evaluation of the process including what worked well during the meeting and what could be improved. Members appreciated the hard work of the sub teams and staff in completing assignment in time for this meeting and the ability of the full team to work toward agreement and respect each other's opinions.

Members suggested an improved phone or speaker system was needed for those who have to call in to participate effectively and that members need to continue to offer suggestions for improvement and avoid getting bogged down in details

Members agreed to adjourn until the next meeting on November 12–14, 2008 in Little Rock, Arkansas.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
Draft Second 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 #2*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*). They also thanked Kevin Sherlin for hosting the meeting at the Sacramento Municipal Utility District offices and for making all of the necessary logistical arrangements.

B. REVIEW OF ANTITRUST GUIDELINES

Harry Tom 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 the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

C. ACCEPTANCE OF ORGANIZATIONAL MEETING MINUTES

Stu Langton and Hal Beardall, with the FCRC Consensus Solutions facilitation team, reviewed the minutes from the first meeting noting several minor corrections for pagination. It was also noted that Bill Winters should be listed as representing Arizona. The group agreed to accept the minutes as they were distributed to the group with the minor corrections noted; however the minutes will be open to additions as necessary. Harry Tom explained that an announcement will go out that the minutes have been posted to the NERC website. It is the responsibility of the members to download the minutes and review them.

D. Planning challenges, Purpose statement & consensus guidelines

Stu Langton provided an overview of organizational issues including the following planning challenges the drafting team will need to keep in mind:

- Organization — a new team testing how best to work together
- Process — using a consensus building approach or process
- Issue Identification — a huge number of issues to identify and organize effectively
- Progression Strategy — important how you organize and address the issues
- Schedule — what is a realistic pace? In what order do we take up issues?

Mr. Langton suggested there are key principles the group should keep in mind to meet the challenges. He noted the group will need the capacity to tolerate ambiguity and patience since the group cannot do everything well all at once and may at times need to wait for more information. The group's progress may be circular as well as linear due to the practical and political variables that must be considered. This will be an iterative process that will build on previous discussions while flexible enough for the group to revisit earlier issues if needed as a result of subsequent discussions.

Following the challenges and principles, Mr. Langton offered for the group's consideration the following draft purpose statement as a starting point for review and discussion:

> "The overall purpose of the Cyber Security of Order 706 SDT is to work together to build consensus on a package of recommended draft cyber security standards and implementation plan that is responsive to and consistent with the scope of the SAR and the FERC Order 706.
>
> The Team's products will seek *to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system* and will be submitted for consideration by the registered ballot body. *(Italics from the SAR "purpose" statement)"*

Team Comments and Questions on the Draft Purpose Statement:

- Is this where we look at changing to "bulk power system" from "bulk electric system"? That is the language in the SAR
- "Critical Cyber Assets"? Using that term limits us to that subject. Do we want to limit ourselves to the critical assets?
- Yes, we do want to limit to those issues
- Also concerned about limiting us to those issues
- Critical Cyber Assets – definition includes assets essential to bulk electric system – can strike the word "critical" here
- In the first paragraph consider replacing with "package of recommended modifications to the cyber security standards"
- Remind group that this is part of the SDT process. The SAR sets the scope of this group to look at revising all of the CIP standards based on the order. You have to look at the standards top to bottom. Be careful, this scope can not limit you
- We need to be on the same page but the SAR already sets the scope of this group. We need to cross reference the purpose back to the scope as set by the SAR. We do not want to redefine the SAR
- Who are we serving? NERC, our companies, the public at large? Who are we doing this for? We could be serving more than one, but we are not serving the balloting body
- Expected to serve the public and the industry not the aspirations of our individual companies. Put that into the draft purpose statement.

The group agreed to the suggestion that the facilitators work with the chair and staff to reframe the scope based on this discussion and bring a new draft back to the full group for review next time

Mr. Langton provided an overview of how consensus could be defined and used by the drafting team *(See Appendix #6)*. He noted that consensus could 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 percent 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.

Team Comments on Consensus Guidelines

- Agreement may not be at the same level to all
- These guidelines call for a 75% favorable vote but the standards committee set rules for 2/3's favorable vote – need to make consistent – quorum requires 2/3's present too
- "Dissenting opinion" not in the standards committee rules – how do we document?
- Not a problem to document as a minority report or opinion
- Even if we have consensus of this group, our companies may turn around and say "no" – we are working as a team for the public and the industry
- Know what your CEO wants
- Who in a company provides comments? Depends on the company, usually a lead person responsible for reliability who may get a corporate view, or you can get multiple comments form one company and can be contradictory
- Clarify that members on the phone are counted in any voting or polling
- Members agree to represent and consult their stakeholder interest groups – represent company, sector and self at the table
- What do you mean "seated at the table"? Staff and facilitators are in an advisory role, members are the voting members
- Only team members may participate in discussion? Everyone is invited to participate in discussion, only the votes are limited to members with a caveat to let chair limit discussion if needed
- Clarify that the polling/rating is limited to members and intended to guide discussion but comments are open to observers too
- Want a gentleman's agreement by observers to limit comments to the media
- At the discretion of the Chair or Vice Chair, the straw man polls can be extended to all participants in the meeting and not just be limited to the team members. Need to make sure to gauge the broader consensus by extending the straw poll to all at the discretion of the chair
- Cannot prevent anyone from talking to anyone else – refer to media relations at NERC as needed
- Cannot prohibit you from speaking – give factual updates on what we are doing, but must note personal opinions of the individual and not representing the group
- Group can become very comfortable with what we are doing so knowledgeable of the issues may lose tract of the broader interpretation
- Add phone participants: mute button, indicate name of speaker, use webex button to indicate you want to comment

Mr. Beardall reviewed a set of ground rules *(See, Appendix #6)* for the meeting including additional items added at the first meeting as follows:

- Additional phone protocols include using the mute button when not speaking on the phone. Do Not use the hold button.
- 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 or use the feature on the WebEx that indicates you want to speak
- Ask team members on the phone to use the same WebEx feature to "raise their hands" for their acceptability ranking as needed

E. Reviewing Sub team Draft of NERC CIP Standard

Mr. Langton reviewed the drafting sub team assignments (*see Appendix 4*) and asked sub team leader Jackie Collett to describe the revisions offered for consideration by the CIP 004 sub team. *(See appendix #5 for link to red-line/underline revisions)*

Sub team changes included:

- Improved the wording
- Took out reasonable business judgment
- Training to be completed prior to granting access
- Personnel risk assessment to be completed prior to granting access
- Added provision that emergency provisions should be handled in accordance with CIP 003.R.1.1.

Team comments regarding proposed changes to CIP 004

- Some members did not like the reference back to a different standard within CIP 004.
- There were questions as to the intent of CIP 003.R1.1. and the reference to the meaning of 'emergency' as it is used in CIP 003.
- One member suggested that the Responsible Entity should have a mitigation strategy if the pre-requisites for access (Training and Personnel Risk Assessment) will not be enforced in an emergency.
- Vice Chair suggested that the modified language should be changed to: "…granted such access, subject to the emergency provisions of CIP 003-2."

Group voted on the following three options for references to emergencies concerning Training and Background Screening Pre-Requisites:

A. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access. (No reference to emergency provisions.)
B. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. (Note: This option includes language included in FERC 706 language specifically.)

C. A personnel risk assessment shall be conducted pursuant to the program prior to such personnel being granted such access except in specified circumstances such as an emergency. Emergency provisions should be handled in accordance with CIP 003.R1.1. (Note: This option includes reference back to CIP 003 Policy within CIP 004 R.2&3 to deal with Emergency situations.)

Vote on accepting the proposed CIP 004 language

Preferences	Option A Above	Option B Above	Option C Above
Voting Members	0	22	2

The facilitators suggested an initial acceptability rating (using the 4-3-2-1 scale) of the preferred option to guide additional discussion and refinement.

Acceptance of CIP 004 Proposed Changes	4	3	2	1
Voting Members and Observers	16	8	2	0

Team comments and suggestions:

- 3: Footnote the language to reference CIP-003
- 3: Industry will not know what to document (addressed in CIP-003, R1.1)
- 3: Needs modifications to CIP-003 for completeness – that will be done in Phase 2
- 3: Needs to reference CIP-003 someplace, not necessarily as a footnote. Could be in the FAQ, a Guideline, a NERC definition, or as specific language in the standards themselves.

- There is a definition of "Emergency" or "BES Emergency" that can be used in CIP-003. Need to add some language regarding life and safety issues. Concern that limiting to this combination might be too limiting.
- The term "emergency" is an issue. Perhaps change the language to contingency, exigent, or exceptional.

- **Conclusions concerning CIP 004**
  - CIP 004 was accepted with the changes to require the Cyber Security training and background screening prior to access and with the inclusion of language concerning emergency provisions in accordance with FERC Order 706 (Option B above).
  - **CIP 003** Policy language will be reviewed/modified by a work group in Phase II, not Phase I.

F. Technical Feasibility Exception proposal

Michael Assante, NERC Chief Security Officer, addressed the group by phone and asked the team to consider addressing the technical feasibility exception as a priority and

possibly as part of Phase I. Mr. Assante pointed to the request from FERC to address this issue and reviewed issues to be considered:

- Develop a set of conditions or criteria for invoking technical feasibility exception
- Oversight of its use
- Want operational and safety considerations and not business judgment.
- Want to see a mitigation plan that achieves the same degree of security
- Wants time limitation on the use of the exception
- Senior manager approval of the exception, mitigation, and remediation time line
- Include audits and appeals of the exceptions
- Need to address confidentiality of the exception documentation
- ERO monitoring of the exception
- Accountability

Team discussion:

- Appreciate the importance of the issue but it will take quite a bit of discussion – adding it to the immediate scope may derail the ability to get the phase I products done and the removal of the business judgment language
- This exception should be a priority issue but after we complete the agenda today on the drafting materials for phase I
- Motion:
  - Motion was made by Chairperson to table the issue of the Technical Feasibility Exception until after the team agenda is completed.
  - In favor = 22 members; Against = 0; Abstain = 1; Not present = 1
  - The issue of Technical Feasibility was tabled until completion of the pre-defined agenda

G. Reviewing Sub team draft of NERC CIP Standard 006

Kevin Perry, as CIP 006 sub team leader, provided an overview of the revisions offered by the sub team in CIP 006 for consideration by the full team: *(See appendix #5 for link to red-line/underline revisions)*

- Removed Reasonable Business judgment
- Changed dates as appropriate
- Minor wording changes which did not alter the substance of the requirement
- R1.6 added that procedures for the active monitoring of escorted persons at all times are required.
- R1.8 added that the Physical Security Plan must be reviewed annually.
- R2. (Note: The prior 1.8 requirement becomes R2 in this proposal. The original suggested language follows:
  - R2. Protection of Physical Access Control Systems — Cyber Assets authorizing and logging access to the Physical Security Perimeter(s) shall:
  - R2.1. Exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall reside

within an identified Physical Security Perimeter or be physically monitored 24x7 by personnel authorized unescorted access.

- R2.2. Be afforded the protective measures specified in Standard CIP-003-1; Standard CIP-004-1 Requirement R3; Standard CIP-005-1 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-1; Standard CIP-008-1; and Standard CIP-009-1.

Initial Team Discussion and Questions:

- R1.6. How does an entity prove that escorts actively monitored persons at all times?
- Do we need evidence? Or Proof? You want evidence such as a manual sign-in book with the name of the escort associated with the visitor. Auditors need to understand that.
- Training and awareness is an essential part of the process. Make sure the escorts know their responsibilities.
- Order 706, Para 432 discusses the need for qualified escorts.
- Up to the auditor to prove that you did not comply. Needs a way to test the control.
- May need a NERC defined term on what escorted is.
- R2.1: what happens with a situation where the system is in use 8x5 and locked up otherwise. Unattended systems need to be within the PSP, HMI systems need to be secured when not in use.
- Does the system need to be in a PSP when not in use?

Initial Acceptability Rating

Acceptance of CIP 006 Proposed Changes	**4**	**3**	**2**	**1**
Voting Members	**10**	**7**	**2**	**0**

Team Discussion following Initial Acceptability Rating:

- Gave it a 2: R2.1, primarily around the issue surrounding the HMIs. Are we locking people into the card reader systems? One system may control everywhere.
- Gave it a 2: R3 is a new requirement that entities cannot comply with by July 1, 2009. Resolved by inclusion of a requirement-specific implementation plan.
- Whether the word 'remote' belongs in the physical access standard
- Define the Access Control System in the glossary. Address multiple systems that integrate together. [Credentialing, identification, authorization, authentication, accounting]

Revised Proposed CIP 006 language:

- R2. Protection of Physical Access Control systems – Cyber Assets that authorize and/or log access to the Physical Security Perimeters(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic mechanisms and badge readers, shall:
- R2.1 be protected from unauthorized physical access
- R2.2 be afforded the protective measures specified in Standard CIP 003-1; Standard CIP 004-1 Requirement 3; Standard CIP 005-1 Requirements R2 and R3; standard CIP 006-2 Requirement R4 and R5; Standard CIP 007-1; standard CIP 008-1; and Standard CIP 009-1.

Acceptability Rating for CIP 006 with Revised Proposed Language:

Acceptance of CIP 006 Proposed Changes	**4**	**3**	**2**	**1**
Voting Members	**15**	**8**	**0**	**0**

H. Review of Sub Team Report on Measures & VRFs

Jerry Freese, leader for the sub team on measures, reported that their team performed a review of the measures, but based on changes prior to today's meeting, they believe there are no changes to the measures in response to proposed changes in CIP requirements.

Todd Thompson reported on behalf of the sub team reviewing VRFs that they believe no changes need to be made at this time.

I. New Implementation Plan for Changes to the Existing Requirements after Phase I Changes

Phillip Huff reported on the progress with the Implementation plan for new or changed Phase I requirements. *(See appendix #5 for link to red-line/underline revisions)* The original proposal was that the additional implementation plan would be expanded by 180 days to allow participants to comply with changed requirements.

- Proposed language: the original proposed effective date discussed for the modifications contained in these standards is the greater of (1) 180 days following approval by the FERC or (2) the number of days following approval by FERC before a Responsible Entity must become Compliant with a requirement according to the associated Compliance Schedule.

Team comments and suggestions:

- 180 days after regulatory approval unless the initial compliance table is already a later date.
- Comment made that all requirements of the eight standards are affected and thus the revised implementation date affects all requirements. Does not necessarily make sense.
- Does the entity still need to march toward compliance with Version 1 once the Version 2 standards have been approved by FERC?
- We have added the RE – what table applies? Table 4? Do they also get an additional 180 days beyond that?

- Side Note: CIP-003, R2 needs to be required for all entities in the same manner as CIP-002.

Based on team discussion, the sub team will make additional edits for consistency with changes made in the body of the document and make conforming changes to the standards as identified in review for creating the table.

J. COMMENT FORM REVIEW

Chairman Jeri Domingo-Brewer reviewed the sub team progress on the comment form: *(See appendix #5 for link to red-line/underline revisions)*

- Background information Section uses language out of the SAR to explain what the team had agreed to
- Summary of Phase I Revisions Section summarizes each of the changes
- Requests for Comments/Questions Section requests feedback from commenters

Team comments and suggestions:

- CIP-004, CIP-006, and Implementation Plan changes need to be updated in the Comment Form.
- How do we handle an industry response that says they do not care what FERC requires, they will not approve the changes?
- May need an educational WebEx prior to comment and ballot.
- Really need a robust communications plan.
- Need to reach out to the CIPC and possibly the Regional Compliance Managers.
- Group accepted that this is a good start on the Comment form

K. TECHNICAL FEASABILITY QUESTIONS

Having tabled the technical feasibility exemption question until the end of the day, the Chair asked members how and when they wanted to address the issue.

Team comments and suggestions:

- Is it reasonable to try to do this in Phase I?
- It will touch most, if not all standards. That will require us to at least revisit the implementation plan.
- It was agreed to table this discussion until the next day and the end of the review of Phase I items.

Members agreed to adjourn for the day.

A. DAY TWO – WELCOME AND AGENDA REVIEW

Chairperson Jeri Domingo-Brewer thanked the members of the sub teams for their hard work and reviewed the progress made by the group yesterday. She stated that today the team would:

- Review work from the remaining sub teams that were not reviewed yesterday
- Hanging issue that the group needs to consider pertaining to CIP 006
- Consider the issue of Technical Feasibility based on the request yesterday from Mike Assante of NERC asking the group to add this issue to the agenda for this meeting.

Stu Langton, with the FCRC Consensus Solutions facilitation team, recognized the many details the group was trying to address, the broad range of expertise they brought to the table and the need to build a common understanding of issues and how to address those issues. He discussed the need for individuals who raise questions or concerns to also offer a proposed solution or alternatives to help the group move forward.

B. Implementation Plan Amendments

Scott Mix, sub team lead, reviewed the work that has been done so far concerning implementation plans for new assets and other situations that will be covered under CIP standards in the future. The work included a summary, a narrative explanation of each category, and a timetable. *(See appendix #5 for link to red-line/underline revisions)*

He reviewed who and when an entity would need to be compliant. He noted three milestone categories:

- **Category 1** entities starting from scratch. Existing Table 4 will be used.
  - ***The first identified Critical cyber Asset for a Registered Entity***
  - 24 months to become compliant and 36 months to become auditable compliant.
- **Category 2** is for an entity that already has a schedule and is doing things but they have identified a newly identified Critical Asset.
  - ***Reclassification or change in status of an existing Critical Asset to a Critical Cyber asset.***
  - Questions were raised concerning how the proposed tables would work when/if the CIP standards apply to nuclear. There was no answer provided at this time as there are many variables which still need to be resolved.
  - Mergers
    - For mergers and acquisitions there is a one-year period to bring the two programs of the different companies into harmony.
    - After that one year and after completing the original CIP compliance tables, they would need to comply with the proposed category 2 timetable.

- **Category 3** deals with new assets within an existing Critical Asset. The assumption is that because you are doing something active and that you do not turn on the asset until you have completed the compliance needs within the construction.
  - ***An existing Critical Asset Replacement, reconfiguration, upgrade, or addition of a relevant cyber Asset associated with an existing Critical Asset.***
  - Construction of an asset (substation, etc.) that will be declared Critical upon activation
  - Replacement or upgrade of a Critical Asset
  - Addition of a Critical Cyber Asset at an existing Critical Asset

Scott Mix Sub reviewed the various time thresholds which the sub team is proposing for compliance with the various situations described in the above categories.

Team comments and suggestions:

- One SDT member suggested that NERC maintain consistency in the implementation plans across all the NERC standards.
- The assumption is that if an entity is planning and constructing a new Critical Asset, CIP security compliance should be part of the construction. If a cyber asset exists but through a change such as load flow analysis becomes critical, the entity is provided time to come into compliance with the CIP standards.
- Evergreen plan – affects entities already expected to be Compliant under their original implementation table.
- Assumes everyone is fully in compliance with CIP-002. New entities registering for the first time will come under Table 4 in the original plan.
- Table is applicable to each registered entity. If a merged company retains the original registrations, then a merging of the CIP compliance programs might not be necessary.
- What about a purchase of an asset as opposed to a company merger. Falls into Category 2. Section describing this scenario needs some clarification since the remainder of the paragraph speaks to a merger scenario.
- Need to grandfather assets already in construction under Category 2.
- Merging of companies – harmonization of compliance programs spans all reliability standards, not just CIP.
- Upgrades and modifications to existing Cyber Assets that cause them to become Critical Cyber Assets needs to include the necessary compliance steps as part of the upgrade.
- SDT is asked to evaluate the new table against some business cases to determine if there are gaps or inconsistencies.
- Should require the entity to perform the Risk Assessment prior to placing a new asset or Cyber Asset into service.
- Need to address business cases in the implementation plan

- **Implementation Plan Discussion**
  - Dave Norton volunteered to write a white paper explaining scenarios and he asked for written and constructive input from team members.
  - Vice Chairman explained 6 different scenarios and how each type of scenario could be gamed by entities.
  - A SDT member asked if the implementation time frames should distinguish between field assets (substations, etc.) vs. control center assets. Some team members did not believe the implementation plan was the place to deal with the differences. Further team thought this may need to be considered in Phase II.
- **Homework Assignment Concerning Implementation Plan + Proposed Comment Form:**
  - Team members are asked for a treatment of example scenarios that summarize the categories
  - The goal is to ask yourself 3 questions and categorize appropriate events
  - Suggestions from the team should be send to the Sub Team before October 29.
  - Staff will email the team the Implementation Plan for their review.
  - Comments should be sent to Scott.Mix@NERC.net
  - The Chair asked that the SDT also review the Comment form and provide input to the Comment Form Sub Team.

C. CIP 006 Un-resolved Issue

An additional proposed modification to CIP 006 R1.6 language was discussed and accepted by the group as follows:

- Continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access.

D. CIP 003 Changes and Discussion

Proposed changes were offered to CIP 003 as follows: *(See appendix #5 for link to red-line/underline revisions)*

> **CIP 003 R2:** Leadership — The Responsible Entity shall assign a single 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.

f. NERC audit compliance staff clarified that the Responsible Entity may be either the Corporation as a whole or may be the Registered Entity functions (GO, TO, BA, etc.).

~~g.~~ **CIP 003 R3.2.** Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures. ~~taken or a statement accepting risk. and/or any residual risk~~

Team comments and suggestions:

Senior Manger:

- Designated by the Registered Entity (registered function)
- Can be the same for multiple registrations (multiple functions)

Exceptions:

- Note that an entity cannot take exception to the regulatory standard, and so the exception would be taken to the entity's own policy. Believe that the flexibility for compensating measures and residual risk was appropriate.
- The NIST technical feasibility material may have language that would be of assistance with the concerns.
- The FERC comment referred more to regulatory compliance rather than compliance with the entity's own policy.
- The reference to acceptance of risk needs to be removed as directed by FERC.
- The issue of removing acceptance of risk is so difficult that it should be moved to Phase II.
- Or the language that provides for acceptance of risk should be removed from the CIP standard.

After reviewing several suggested changes, members were asked to rate the language as revised above striking "or acceptance of risk":

The SDT 1st initial rating on acceptance of the proposal.

Scale	4 – Acceptable as it	3 – Acceptable with minor concerns	2 – Not acceptable unless major concerns are addressed	1 – Not acceptable
Voting on the above by SDT	11	7	1	0

Following additional discussion, members were asked to rate the proposal again without the word "any" before "compensating measures:

The SDT 2nd vote on acceptance of proposed language change.

Scale	4 – Acceptable as it	3 – Acceptable with minor concerns	2 – Not acceptable unless major concerns are addressed	1 – Not acceptable
Voting on the above by SDT	12	6	4	0

Following additional discussion, members agreed to retain the word "any"

There was general agreement around the room that in CIP 007 wherever the phrase "acceptance of risk" appears, it will be removed even though each such instance where the phase appears may not have been discussed at length.

E. Proposal to Substitute "Prudent Judgment" for "Reasonable Business Judgment"

Member John Varnell requested the group consider substituting the term "prudent judgment" in place of the term "reasonable business judgment."

Team comments and suggestions:

- The concern is that the cost to remediate the last few percentages of risk could be cost prohibitive.
- FERC believes, in the order, that "reasonable business judgment" is not required to address that issue
- It was pointed out that Paragraph 132 of FERC order states that there is no recourse needed to substitute another term concerning judgment.

Due to a lack of support, the group decided not to move forward with the replacement of the term "reasonable business judgment" with 'prudent judgment."

F. Proposed a Definition of Access Control System

As requested by the drafting team, Scott Mix offered a draft definition of Access Control System as follows:

> A system which provides for Authorization, Authentication, and frequently Accounting of access through either a Physical Security Perimeter or an Electric Security Perimeter. An Access Control System may be a single computer system which performs all three functions or may be a combination of two or more computer sub systems which work together to accomplish all three functions.
>
> - Authentication is the process of verifying a users or object's identify.
> - Authorization is process for granting an authenticated user or object's the authority to perform a certain operation.
> - Accounting provides an audit trail of access, and includes logging of access by identification and time.

Team comments and suggestions:

- Needed to provide clarity to CIP-005 and CIP-006
- Will help industry understand the concept.
- Does not include a credentialing system.
- Should be a requirement around the credentialing system.
- The SDT was asked to submit their comments for the resolution of preferences concerning the definition to Vice Chair, Kevin Perry.

G. Technical Feasibility

The Chair that there were two potential proposals (one from Scott Mix and one from Keith Stouffer) for addressing "technical feasibility" exception in Phase 1. She asked the team to listen to each of the proposals, consider the proposals, and decide if one of the alternatives offered could be included within the Phase I work of this team.

- **Scott Mix reviewed material directed in the FERC Order 706**
  - All requirements in a NERC standard must be adhered to
    - Implies no exception
  - Self report a non-compliance (exception) with Mitigation Plan is allowed
  - Commission views the term 'acceptance of risk' as an uncontrolled exception
  - Alternative language that deals with such issues in terms of technical feasibility is preferable.
  - Flexibility along with control is the goal.
  - FERC does not support the long established practice of risk acceptance by sr. management
  - FERC wants specific framework for invoking the technical feasibility provisions
  - FERC narrows the application by stating that there are acknowledged concerns (device will not support) compliance with the requirement
  - For future installations the technical feasibility would not carry forward. New equipment should be compliant.
  - FERC steps
    - Comparable level of security to the requirement
    - A remediation plan although a date certain is not required for replacement
  - Exemptions should be reports, justified, and approved by the ERO or relevant Regional Entity
  - Regional entities should catalog notices of technical feasibility
  - Actual evaluation and approval of technical feasibility exceptions should be performed
  - Technical feasibility should be audited
  - NERC must protect such information
  - FERC wants a framework includes mitigation steps, regular review, justification, internal approval by the senior manager, wide area approval through the ERO audit process, and cooperation with the ERO to provide the Commission with high level impact of the technical feasibility on the reliability of the grid.

- **Keith Stouffer of NIST provided an alternative proposal on Technical Feasibility**
  - This is addressed within the NIST framework for risk management
  - The Responsible entity may invoke a technical feasibility exception to a requirement is any of the following conditions apply:
    - The requirement poses a risk to the reliability of the Bulk Power System

- The requirement creates a significant adverse effect on operations and/or safety impact
- The requirement specifies mechanisms or functions that are not technically possible for a cyber asset to support

- The responsible entity shall document all Technical Feasibility exceptions in an Exception Plan containing:
  - A justification why the Technical Feasibility exception is necessary
  - Compensating controls or mitigation steps that provide a comparable level of security
  - A plan of action, milestones, and schedule for implementing the compensating controls.
  - Obtain approval by the senior manager
  - Approval by the Regional Entity or the ERO
  - ERO must annually audit compliance with the Exception plan
  - ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System
  - Keith proposed that this section may be included before the effective date

- Scott Mix also reviewed the current Self Reporting Process. Based on the similarities between FERC directives and the items required by a self reporting of non-compliance, Scott suggests that this same process be used for Technical Feasibility Exceptions:
  - Document non compliance to a specific requirement
  - Provide explanation
  - Describe reliability impact
  - Describe any external or extraneous factors
  - Provide mitigation plan
  - Provide mitigation schedule
  - Obtain Senior Officer signature
  - Catalog and approval by ERO
  - Catalog and approval by Regional Entity
  - Submit to FERC (US Entities)

Scott Mix reviewed similarities between the proposals:

Keith Proposal	Scott Proposal
A justification why the Technical Feasibility exception is necessary	Document non compliance to a specific requirement h. Provide explanation i. Describe reliability impact j. Describe any external or extraneous factors

Compensating controls or mitigation steps that provide a comparable level of security	
A plan of action, milestones, and schedule for implementing the compensating controls.	Provide mitigation schedule Provide mitigation plan
Obtain approval by the senior manager	Obtain Senior Officer signature
	Catalog and approval by Regional Entity
ERO must annually audit compliance with the Exception plan	Catalog and approval by ERO May trigger accelerated audit schedule Annual review and re-approval by Responsible Entity and ERO
ERO to provide FERC with a high level assessment of the exceptions on reliability of the Bulk Power System	ERO to develop separate annual report to FERC Analyze the combined impact of all Technical Feasibility exemptions
	Report will contain sensitive information – must be CEI protected
	Submit to FERC (US Entities)

Team comments and suggestions:

- **Information Protection Concerns**
  - Concern was voiced about the controls over protection of the information that would be supplied
  - The specific detail regarding the exception should stay with the asset owner.
  - NERC has not yet addressed the confidentiality issue to any great extent
- **Proposed Whitepaper on Technical Feasibility**: draft and submit to the industry a high level concept document on Technical Feasibility simultaneously, but not as part of a revision to the standard in Phase I. Offer the industry a comment period to react to this as a concept to be folded into a standard later.
  - Allows the regions to review and respond to the proposal.
  - Allows time for NERC to assure protection of the information to be provided.
  - Questions arose concerning whether the technical feasibility exception applied to all requirements or to only certain of the requirements.

- **Proposal** Prepare a 'conceptual' document to seek stakeholder consideration and feedback that describes a Technical Feasibility Exception process that parallels existing compliance self report process.

Scale	4 — Acceptable as it	3 — Acceptable with minor concerns	2 — Not acceptable unless major concerns are addressed	1 — Not acceptable

1st Poll — Voting SDT	20	2	0	0

Additional Team comments and suggestions:

- Need to address issue of information protection in the proposal
- Who will be involved?

Next Steps for Technical Feasibility "White Paper":

- Proposal Sub Team: Tom Hofstetter, John Varnell, Keith Stouffer, Scott Mix, Jerry Freese and possibly someone from NERC compliance.
- Due for the next full team meeting

H. Assignments and Next Steps for the Next Meeting

1. For the next WebEx, October 29:

- NERC staff needs final products by cob Monday, 27th to distribute on Tuesday
- NERC staff will provide progress report on Draft proposal concerning technical feasibility
- Implementation Plan for new CA/CCA — should be done and distributed prior to October 27
- Implementation plan (CIP Version 2)
- Final Comment Form on the 28th
- Final versions of CIP 004 & CIP 006 language

2. Notes on Future Meetings and Proposed Topics

- Webex, November 3 — develop concept document for Technical Feasibility. Deliver to full team by November 7 or 10.
- Webex, November 5 – following NERC Staff feedback, review and conform drafts per feedback.
- November 12–14 — full team meeting in Little Rock, Arkansas to Finalize Phase I documents as needed and review proposed roadmap
- December 4 or 5 — In person meeting at FERC Offices in Washington DC
- January 7–9 — In person meeting at APS in Phoenix, AZ

3. Roadmap Proposals and Discussion

The Chair suggested that in December the group may begin to hash out the large issues still to be addressed. She cautioned members to think outside the box when it comes to all of the work to be done in the future.

The Vice Chair offered two alternatives to the "Roadmap" going forward, a multiple phase or single phase approach.

Multiple Phases:

- Phase I — Issues defined

- Phase II — Technical Feasibility Exception
- Phase III — Risk Assessment framework (18-24 months from end of Phase I). Overhaul CIP-002. Review future phases at that point for CIP-003 through CIP-009. Consider breaking apart the standards into Generation, Transmission, Control Centers, and Special Protection Controls.

Single Phase II:

- Phase II is everything not in Phase I
- Would be continuously communicating with the industry during the development time
- Can choose to post work once majority is completed in the event there are a couple of really difficult issues still on the table.
- Expect to have everything nailed down within 18 months of Phase I.

The Vice Chair made a proposal that the SDT should use an incremental approach.

Team comments and suggestions:

- Nothing sacred about 8 standards.
- If we are going to fundamentally change the standards, we do not want to dribble them out.
- Really intriguing concept to break out the standards functionally rather than one size fits all.
- At some future date we need to have the strategy planning session to determine how we approach the task at hand.
- Does there need to be a training of the industry as part of the strategy?
- Everything is an iterative process – determine next step as you finish up the current step.
- We are concerned with control systems, not information systems. Need to bear that concept in mind as we move forward.
- If we are going to make a revolutionary change, we need to start chewing on that now.
- We are starting to look more and more like traditional IT systems (Off The Shelf solutions are now proliferating).
- The integrated nature of systems is a real issue. We have to figure out how to deal with distribution and home network systems since they interconnect with the transmission-level systems. Also need to consider and handle interdependencies of critical infrastructures.
- Do we have enough representation on the team regarding distributive control systems? Need someone with ISA experience or expertise.
- Probably going to need a couple of days to hash out the strategy. Focus on work plan now and the strategy in January.
- Should address early on the requirement to address the FERC issue of compromised systems (used for malicious control).

- Need to resolve the information protection issues for the required external review of Critical Assets.
- When are we going to address Physical Security of the Critical Assets?
- One of the 17 control families in NIST is physical security controls.
- Pending legislation that will bring distribution systems into the critical infrastructures.
- Do we need a CIP-010 to address emergency actions?
- What are the implications for when the standards apply to the nuclear side of the house?

The FCRC Consensus Solutions facilitation team were asked to develop a one page proposal (big picture straw proposal and guiding principles) for addressing the remaining issues following Phase I for review and discussion by the full group at the next meeting in Little Rock, Arkansas. Member discussion today has included several key principles that could guide development and discussion of remaining issues.

4. Review of Remaining "Parking Lot" Issues Identified at the First SDT 706 Meeting

"Parking Lot" Issue:	
Emergency	Phase II item
Define Cyber Security Incident	Phase II item
006 SCG&E interpretation	Phase II item
Audit against policy question Industry concern regarding CIP 003 language that says the Responsible entity shall document & implement a cyber security. If the policy or sub documents exceed the CIP standards in depth or in scope, there is a desire within the industry for NERC to clarify that if they are in conformance with the CIP standards but fall short of their policy implementation, they should not be held in non-compliance. Auditors are asking the industry to demonstrate that they are in compliance.	NERC compliance staff have stated that they will audit to the standards
Communications Plan	In the future regular updates to regulators, and industry stakeholders will be necessary.

I. What Worked and Did not work

At the conclusion of the meeting, the facilitators asked the Team to offer an evaluation of the process including what worked well during the meeting and what could be improved.

What Worked Well:

- Prep work of the sub teams
- Need to improve the sound on the Web ex's for those who are not attending in person
- Talking about issues in a general way instead of the individuals' corporation perspective
- NERC staff offered feedback that they are pleased with the progress that is being made by the SDT
- Detailed agenda
- Assignments were completed prior to the meeting
- No picking holes – offered improvements
- People left their company hats at the door more often
- Refrained from violent agreement
- Many thanks to Kevin Sherlin and SMUD for hosting the meeting
- While we may have issues, this group has made excellent strides reaching consensus on our issues. Much more productive than most other teams.
- Scott and Harry have done a lot of pre-work and evening work to keep the team making progress.
- We all respect each other and agree to disagree
- External facilitation is essential
- Phase I is NOT a toothless tiger as had been feared.

What Could Be Improved Work

- Phone system is difficult. Hard to hear and follow the meeting
- Need to identify speaker when starting to speak
- Seemed bureaucratic at times
- When offering feedback, speakers should offer improvements not just pick on proposals
- On a couple of occasions the SDT got bogged down in details
- Need to facilitate toward resolution rather than getting bogged down in details.

Members agreed to adjourn until the next meeting on November 12-14, 2008 in Little Rock, Arkansas.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 1

Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

October 21, 2008 | 8 a.m.–5 p.m.
October 22, 2008 | 8 a.m.–5 p.m.
Sacramento Municipal Utility District
6301 S Street
Sacramento, California

Day 1 Agenda

1. **8 a.m. — Opening Remarks — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair**
   a. SMUD Welcome — announcements, logistics
   b. NERC Antitrust Compliance Guideline
   c. FSU/CRC review of last meeting and adoption of meeting summary
2. **8:15 a.m. — SDT Organizational Issues: Purpose Statement and Adopt Rules of the Road**
3. **9 a.m. — Presentation and Review of Phase I Drafting Group Products**
   a. (Requirements, Measures, Implementation Plan, Comment Form, VRFs)
4. **10:15 a.m. — BREAK**
5. **10:30 a.m. — Phase I presentations and review — continued**
6. **noon Lunch — working (return to meeting at 12:45 p.m. ET)**
7. **12:30 p.m. — Phase I presentations and review — continued**
8. **3 p.m. — BREAK**
9. **3:15 p.m. — Review of Assignments to Finalize Phase I Redline Versions**
10. **4:45 p.m. — Review of Progress and Adjustments, as needed, Day 2 Agenda**
11. **5:00 p.m. — Recess**

Day 2 Agenda

12. **8 a.m. — Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair and Kevin Perry, Vice Chair**
13. **8:15 a.m. — SDT Organizational Issues (TBD)**
14. **8:30 a.m. — Post Phase I (Phase II) Project Roadmap — discussion**
    - Review of CIP 002-009 — Identify Approach, Key Issues from FERC Directive including NIST comparison, etc.
15. **10:30 — BREAK**
16. **10:45 — Continue Review of CIP 002-009 — Approach, Issues from FERC Directive including NIST comparison**
17. **noon — Lunch — working (return to meeting at 12:45 p.m. ET)**
18. **12:45 p.m. — Review of CIP 002-009 — Approach, Issues from FERC Order including NIST comparison.**
19. **2:45 p.m. — BREAK**
20. **3 p.m. — Post Phase I Project Roadmap — discussion, continued**
    - Disposition of RFI from SCE&G and U.S. Army Corps of Engineers
    - Review of Parking lot items from Gaithersburg meeting or Day 1
    - Initial Phase 2 Schedule Structure
21. **4:15 p.m. — Review of short term meeting schedule and Post Phase I drafting assignments**
22. **4:45 p.m. — Next Steps and Evaluation**
23. **5 p.m. Adjourn**

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 2

Cyber Security for Order 706 SDT Attendees List
Project 2008-06 — CS 706 SDT
SMUD — Sacramento, CA
October 21, 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. Sharon Edwards	Project Manager, Duke Energy
4. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
5. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
6. Tom Hoffstetter	Midwest ISO, Inc
7. Philip Huff	Arkansas Electric Cooperative Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. of New York
10. David Norton	Policy Consultant, CIPEnergy Coporation
11. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16. Keith Stouffer	National Institute of Standards & Technology
17. Michael Winters	Arizona Public Service Co.
18. William Winters	Hydro One Networks, Inc.
19. David Taylor	NERC
20. Harry Tom	NERC
21. Roger Lampila	NERC
22. Scott R. Mix	NERC
23. Todd Thompson	NERC
24. Hal Beardall	FSU/FCRC Consensus Center
25. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx

1. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
2. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
3. Jackie Collett	Manitoba Hydro
4. Scott Rosenberger	Luminant Energy
5. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis

Attending in Person — Participants

1. James Brenton	ERCOT
2. Michael Toecker	Burns & McDonnell Engineering

Attending via WebEx — Participants

1. James Bassett	IPC
2. Marcus Braendle	ABB
3. Steve Brezina	WAPA
4. Jerome Farquharson	Burns & McDonnell Engineering
5. Mike Mertz	Southern California Edison
6. Matt Schnell	Nebraska Public Power District
7. Karen Yoder	First Energy

List of Attendees — Cyber Security Order 706
Standard Drafting Team Meeting
SMUD — Sacramento, CA
October 22, 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. Sharon Edwards	Project Manager, Duke Energy
4. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
5. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
6. Tom Hoffstetter	Midwest ISO, Inc
7. Philip Huff	Arkansas Electric Cooperative Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. of New York
10. David Norton	Policy Consultant, CIPEnergy Coporation
11. Kevin B. Perry, Vice Chair	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Jonathan Stanford	Bonneville Power Administration
16. Keith Stouffer	National Institute of Standards & Technology
17. Michael Winters	Arizona Public Service Co.
18. William Winters	Hydro One Networks, Inc.
19. David Taylor	NERC
20. Harry Tom	NERC
21. Roger Lampila	NERC
22. Scott R. Mix	NERC
23. Todd Thompson	NERC
24. Hal Beardall	FSU/FCRC Consensus Center
25. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx

1. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
2. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
3. Jackie Collett	Manitoba Hydro
4. John D. Varnell	Technology Director, Tenaska Power Services Co.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis
2. Scott Rosenberger	Luminant Energy

Attending in Person — Participants

1. James Brenton	ERCOT
2. Michael Toecker	Burns & McDonnell Engineering

Attending via Webex — Participants

1. Haung Ngo	Reliant
2. Karen Yoder	First Energy

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 participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

Appendix # 4

Assignments from First SDT 706 meeting (Gaithersburg, MD)

	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 associated with changes in CIP-002 to CIP-009	Jerry Freese	Keith Stouffer, Roger Lampila, Todd Thompson	Straw Proposal due to 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

Appendix # 5

Below is a link to the presentations and all of the documents reviewed as part of the SDT 706 Sub Team Reports with red-lined/underlined revisions proposed by Sub Teams and further revisions agreed to during the full Team discussions in Sacramento:

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #6

Standard Drafting Team Draft Consensus Guidelines

October 21–22, 2008

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

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**
  - Members in the room should use name tents to be recognized to speak
  - Telephone participants should give their name and indicate desire to speak on the topic

- **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