NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

November 12, 2008 | 1–5 p.m.
November 13, 2008 | 8 a.m.–5 p.m.
November 14, 2008 | 8 a.m.–noon
Arkansas Electric Cooperative Corporation Offices
Little Rock, Arkansas

Meeting Facilitation and Draft Report By:
Robert Jones, Stuart Langton, and Hal Beardall

FCRC Consensus Solutions, Florida State University

Thanks to Team members Sharon Edwards and Kevin Perry for their meeting notes.

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

MEETING SUMMARY CONTENTS

EXECUTIVE SUMMARY

The Chair, and Vice Chair welcomed the members reviewed with the team and participants the proposed meeting agenda and thanked Phil Huff for hosting the meeting at the Arkansas Coop offices. Harry Tom reviewed with the team the need to comply with NERC's Antitrust Guidelines. The team accepted the October draft meeting summary but agreed that it will be open to editorial corrections as necessary.

The team reviewed and unanimously adopted the consensus guidelines which had been revised since the Sacramento meeting to address consistency with the NERC Reliability Standards Development Procedure.

Following discussion, the team unanimously adopted the following SDT purpose statement:

> The team is serving the public interest throughout North America to protect the critical cyber assets that include hardware, software, data, and communications networks essential to the reliable operations of the bulk power system.
>
> The team's outcomes will be achieved by working together to build consensus on a technically sound and complete package of recommended draft cyber security standards and realistic implementation plan that is responsive to and consistent with the scope of the SAR, the FERC Order 706 and the ANSI process.

Following an overview and extensive discussion of how to address the proposed edits by the NERC Standards Process Manager, and a review of specific edits in CIP 00 and 003, the SDT decided to accept agreed upon "global changes" discussed in CIP 002-003 review and reject all other changes reverting back to the final Sacramento language version. Team member Jackie Collett presented CIP 002-009 global revisions, including CIP 006 revisions made by Kevin Perry, for consideration by the team. The team also accepted the Implementation section language as revised on November 13 by the sub-team.

In the review of the Newly Identified Assets Implementation plan the team unanimously agreed to go back to the Sacramento agreed-on approach and have the "newly identified asset" CCA implementation plan as a separate document with no changes in the existing CIP standards documents to be posted for industry comment with Phase 1 documents. Based on comments from Phase I industry review and experience in the field, the SDT will consider incorporation into the standards documents in Phase II. The SDT will ask the industry whether they think it should be incorporated into the CIP standards documents as part of the Phase I submission for vote. Following the poll, Scott Mix made conforming changes in the draft language and the SDT then unanimously agreed to move forward this as a separate paper in Phase 1.

Jeri Domingo Brewer reviewed the SDT sub team's revisions to the comment form based on the revisions to the standards adopted by the team and the SDT unanimously agreed to adopt the Comment Form at part of the Phase 1 documents.

On Friday morning, the SDT Phase I package of documents was moved for adoption and submission to the industry for comment (Mover: Kevin Perry, second: Sharon Edwards). The Phase 1 Package was adopted unanimously without discussion.

The SDT reviewed the Phase II options paper drafted by the facilitators with input from the Chair, Vice Chair and some SDT members. The facilitators presented some initial draft assessment criteria and invited the SDT to clarify, revise or add additional criteria. The facilitators suggested the criteria could help provide a frame for each member to assess the acceptability of the various options for how to proceed. Below is the second draft of the assessment criteria:

SECOND DRAFT PHASE 2 OPTIONS ASSESSMENT CRITERIA
(Not Weighted nor Prioritized)

Initial Draft Criteria as Revised by SDT in November 14 Discussions

A. The option is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
B. The option is achievable given the SDT schedule and work plan.
C. The option does most to advance and enhance cyber security.
D. The option helps the SDT address the foundational issues with the current standards.
E. The option is capable of implementation.
F. The option is capable of improving compliance.

New Criteria Identified by SDT in November 14 Review

G. The option helps protect the current investments and wherever possible builds on what has already been done.
H. The option helps to identify and mitigate risk on an ongoing basis.
I. The option balances a systems orientation with a facilities orientation to asset protection approach. The option is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
J. The option enables the industry provide the appropriate level of security (not over securing nor under securing the cyber assets).
K. The option allows for discrimination among the various types of infrastructure that supports the BES.

The SDT then discussed, refined and reduced the number of optional approaches to four for consideration. The team ranked the acceptability of four identified options for going forward and then directed the Chair, Vice Chair and facilitators to design the December agenda around the approach receiving the greatest support from team members. Below are the results of that exercise:

PHASE II WORK PLAN OPTIONS IN RANK ORDER
(As identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**9**	**5**	**4**	**0**	**3.27 of 4**

2. Adopt/adapt NIST into CIP or Merge NIST into CIP

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**3**	**9**	**4**	**0**	**2.93 of 4**

3. Revise CIP as directed — leave as is and add in only items identified by FERC order

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**5**	**7**	**7**	**0**	**2.89 of 4**

4. Start Over — in terms of a starting point

Acceptability Ranking Scale	**4** = acceptable, I agree	**3** = acceptable, I agree with minor reservations	**2** = not acceptable unless major reservations addressed	**1** = not acceptable	**Avg.**
11-14 rank	**2**	**5**	**7**	**5**	**2.21 of 4**

Scott Mix reviewed the "Technical Feasibility eight page document with two pages included of questions which were reviewed at the Sacramento meeting. This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round to send to the SDT for review prior to December. He noted the goal would be to post a paper approved by the team for comment soon after the December meeting. The comment period would overlap with the Phase I period but would last longer.

In reviewing next steps, the SDT reviewed the status of the NERC Phase I communication plan and asked for a presentation at the December meeting. They also reviewed the Phase I schedule and evaluated what worked in Little Rock and what could be improved going forward. The proposed December agenda items included:

- Review elements of communication plan for Phase I
- Technical Feasibility review
- Background on NIST and its application
- Continue discussion of Phase II approach

Members agreed to adjourn at 11:30 a.m. on Friday until the next meeting on December 4–5, 2008 in Washington D.C.

Cyber Security Order 706 Standard Drafting Team
Draft Third Meeting Summary

I. 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 Phil Huff for hosting the meeting at the Arkansas Coop. offices and for making all of the necessary logistical arrangements.

II. 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.

III. Acceptance of Second SDT Meeting Summary

On Wednesday the Chair asked members to review the October draft meeting summary and the team would seek to adopt it on Friday. On Friday the Chair reviewed the minutes from the second meeting. The Chair suggested and the team agreed to accept the minutes as they were distributed, however the minutes will be open to editorial corrections as necessary. The Chair noted that an announcement that the minutes have been posted to the NERC Web site will be sent to members and other participants. It is then the responsibility of the members to download the minutes and review them in advance of meetings.

IV. SDT Consensus Guidelines

The team reviewed the consensus guidelines *(Appendix #5)* which had been revised since the Sacramento meeting to address consistency with the NERC Reliability Standards Development Procedure. The facilitator noted that the consensus process and techniques were designed to produce as close to 100 percent support of the team's final products as possible. The team discussed what level of agreement it should establish for making final decisions on substantive proposals. They agreed that it will be essential to seek as much consensus support among the team of its proposals since the products will be scrutinized and tested by the industry, many of whom may not be cyber security subject matter experts. Some noted that the initial adoption of the voluntary CIP standards was a controversial and challenging process and that the passage of mandatory cyber security standards will be at least as challenging. The team agreed to set its threshold for team decision making at least a supermajority of 75 percent of the SDT members. The Chair pointed out this exceeds the two-thirds vote needed to approve a standard by the ballot body.

The team also agreed to adopt a quorum rule of two-thirds of the team's members present in order to make decisions. This is consistent with the quorum set forth in the NERC rules for the ballot body process. Finally the team agreed to provide a statement consistent with the NERC

procedures that voting may take place in the context of formal SDT meetings or may take place through electronic means. The team unanimously adopted the consensus procedures as revised.

V. SDT Purpose Statement

Mr. Langton noted that the Chair and Vice Chair worked with the facilitators to respond to the range of team comments on the first draft purpose statement reviewed at the Sacramento meeting. The following revised purpose statement was offered for the team's consideration:

> **The team is serving the public interest throughout North America to protect the critical cyber assets that include hardware, software, data, and communications networks essential to the reliable operations of the bulk power system.**
>
> **The team's outcomes will be achieved by working together to build consensus on a technically sound and complete package of recommended draft cyber security standards and realistic implementation plan that is responsive to and consistent with the scope of the SAR, the FERC Order 706 and the ANSI process.**

In the discussion that followed, the team acknowledged the issue of communications networks as part of the range of critical cyber assets that need protection. Some emphasized that the team's focus should be on the data that moves over the system and not just on the facilities in the bulk power system. Following the discussion, the team unanimously adopted the SDT purpose statement.

VI. Review and Adoption of Phase One Products

A. Introduction and Overview of NERC Edits

David Taylor reviewed with the team the process for reviewing the team's draft products. He noted that the Standards Process Manager who works on behalf of the Standards Committee. This review as not intended to be a substantive review of the requirements but a fresh review "from the outside looking in" of the proposed SDT language for the standard requirements and other Phase 1 documents, with an eye towards compliance issues. For example, the term "risk based assessment methodology" may need some clarification and perhaps there is an alternative choice of word, better accepted and understood by all who would be reading this. Team members also felt strongly that the SDT's language: "This standard, in conjunction with the other standards in the set CIP-002 through CIP-009, comprise a cyber security framework for the protection of Critical Cyber Assets supporting the reliable operation of the Bulk Electric System," was critical to the draft and should not be removed as suggested by the NERC Standards Process Manager.

B. Team Review of Procedural Approaches to Reviewing Edits

The team discussed how to address NERC's Standards Process Manager proposed edits of the Phase 1 draft documents the team unanimously adopted at the conclusion of its October 21–22 meeting in Sacramento. Due to tight timeframes, an interim WebEx call scheduled to review the proposed NERC editorial changes was canceled. Many of the team members and sub teams did not have a chance to review the proposed edits in

advance of the meeting. After extensive discussion, the team identified and conducted a poll on the preferred approach to finalizing Phase 1 products.

Proposed Approaches	SDT Preference Poll
1. Review 002-009 spending ten minutes on a section. If not resolved, default to final draft as proposed by SDT. If six or more members reject the proposed edit, we reject the proposed edits go and go on to the next requirements.	**11**
2. Reject NERC Standards Process Manager's Changes	**8**
3. Table the discussion of NERC Standards Process Manager's changes. Focus on Requirements first, then Data Retention. We will not be concerned with boiler-plate standards changes made by NIDR.	**1**
4. Leave Alone - Deal with Implementation Plan and other substantive issues. After we do that we consider NERC Standards Process Manager's changes.	**0**
5. Accept NERC Standards Process Manager's changes	**0**
Total	**20**

The team agreed to utilize the approach to go through CIP-002 and touch each change briefly to determine whether to accept or reject, but then to check on its efficacy in moving through the proposed edits and reviewing new language for other products.

C. Initial Review of CIP 002-003

The team's efforts for the rest of the afternoon addressed whether to accept the range of proposed edits by the NERC Standards Process Manager. A chart reflecting the team's day one decisions is displayed in *Appendix #6.*

D. Agreement on Global Edits and Retention of the SDT Requirements and Measures

Following the Team's review of proposed edits to CIP 002, 003 and part of 006, it decided to conduct a ranking of options in going forward with their review. They tested the support for the two proposals noted below.

Proposal	Initial Straw Poll	
1. Accept agreed upon "global changes" discussed in CIP 002 and 003 review — Reject all other changes. Other than global changes, this reverts all standard language back to Sacramento version	20 Y	4 N

2. Accept global changes plus what was already done on CIP 002 and CIP 003. Reject everything else.	Not passed

Team Comments after Poll

- Concern that we are rejecting the changes we made in 002 and 003; which says something about our process?
- Understand the comment but 2 and 3 are really overall governance standards and we are not comfortable accepting the proposed edits without reviewing and reflecting on all the changes to each section.
- Concerned that some changes in 2 and 3 may impact the others without further review.
- This process was not a waste of time; the team had a good and necessary discussion that sets the stage for future work.
- We went through a necessary exercise and valuable team exercise, we then reflected and adjusted based on the experience.

	2nd Poll	
1. Accept all agreed upon global changes — Reject all other changes and edits proposed by NERC Standards Process Manager. Other than the global changes, this reverts all standard language back to the version adopted at the conclusion of the Sacramento meeting.	23	2
2. Accept global changes plus what was already done on CIP 002& CIP 003. Reject everything else.	*Failed to get enough support*	

Review of Global Edits

Team member Jackie Collett presented CIP 002 through CIP-009 global revisions, including CIP-006 revisions made by Kevin Perry, for consideration by the team.

E. Implementation Plan

Phillip Huff reviewed the SDT sub team's suggested revisions and agreed following comments to meet with the Sub team to address suggestions for revisions.

Comments:

- Did compliant date get changed? The "Introduction" makes clear that compliant date is not important.
- If use effective date in the standards then need to include here for consistency.
- Do we need to spell out the "versions" to avoid confusion?
- Also capitalize "Implementation Plan".
- Version 1 is the original 706 standard use "version one" in () to shorten subsequent references, similar description and use of version two.

- The second paragraph was offered by the sub-team for explanation but can dropped if the language is considered too informal.
- What does "Auditable compliant" mean?
- If compliant with standard on day one then do not need years worth of documentation — semantics — agree with having one date and that it does not mean that you will have one years worth of documents on that date.

Following a sub-team meeting over lunch, Mr. Huff reviewed the change proposed for the effective date.

Comments

- Is this to be inserted in place of specific item or as a global item in all the standards? As a global item in all the standards.
- Place it in the effective date for each standard.
- Both options to be included to offer option — not offered here as to which one to include in the standards.
- Why not say 180 days? NERC wants the compliance dates to line up with quarters to make auditing easier.
- The SDT discussed moving the parenthetical but left in as boilerplate already given to the drafting team. The parenthetical is meant as a clarifier not an alternative — remove the "or" in the parenthetical to clarify?
- Change to capital "Compliant Date"? That means it needs to be in the glossary — leave in lower case.
- Is this the effective date that appears in the footer of the document (XXXX)? No that footer addresses when FERC ultimately approves.
- It would have to be read multiple times to understand.
- The later of: i); or, ii) ….
- Remove "applicable"? Leave in to cover different Canadian jurisdictions.

	Poll of SDT Members	
Accept the Implementation section language as revised on Nov. 13	19	1

Comments following the Poll

- Still confused as to when this could become effective to investor owned utility in the U.S.?
- Possibly the end of next year.
- Note this is not the newly identified asset "implementation" plan.

F. Newly Identified Assets — Implementation Plan

Scott Mix reviewed the suggested revisions noting the new requirement R3.1.

Comments on Proposal

- Is this something we need to move here — identify senior manager — We agreed in Sacramento to include senior manager?
- Should say first calendar "day" of the first quarter.
- If categorization of an asset is now required is it subject to audits? As a requirement the answer is yes but how? Need to give compliance a chance to review.
- Should we be wrapping into the standards as a requirement in Phase 1 as opposed to a white paper for comment? We discussed in Sacramento and agreed to the white paper approach.
- Categorizing the equipment support reliable operation? This is about compliance first, not operations.
- CIP-002 has a new requirement CIP-003 through 009 do not
- Are we asking for a world of hurt by adding additional verbiage? This would add a lot of text to the standards here. Yes, but this is really salient concern in the industry asking us to fix this.
- Suggestion is not to not include it but address it as a separate document rather than embed in the standards
- Give ourselves a waiver under the applicability standard; avoids complications under implementing, and it is still auditable, but allows equipment to avoid compliance for longer period of time.
- How does it get implemented without embedding it? It gets a two-year test run as a separate document and in phase 2 we use the comments and practice and adjust as needed into the standards.
- Separate document makes it clearer what the concept is that is being presented to the industry.
- Give a 180-day waiver to critical and 30-day waiver for non-critical? Time could be adjusted, but it gives industry time to adjust to the concept before implementation.
- Simplicity is appealing but could be wrong — this is a complex issue that needs a complex answer to address multiple permutations — industry will tell us which ones are wrong.

The SDT used a straw proposal acceptability ranking to test support on how to proceed:

Consensus Ranking on options for how to present the "Newly Identified Assets" Implementation plan	**Acceptability Rank**			
A Go back to the Sacramento agreed on approach and have the "newly identified asset" CCA implementation plan as a separate document with no changes in the existing CIP standards documents to be posted for industry comment with Phase 1 documents. Based on comments from Phase I industry review and experience in the field, the SDT considers	**4**	**3**	**2**	**1**

incorporation into the standards documents in Phase II. Ask the industry whether they think it should be incorporated into the CIP standards documents as part of the Phase I submission for vote.	**19**	**2**	**0**	**0**
B. Instead of option A above, address the new assets within the applicability section	**3**	**9**	**8**	**1**
Poll on Support for Proposal A	**Poll**			
Who accepts Proposal A?	21-0			

Comments after the Poll:

- Need to strive for consistency where ever possible; have to look at different parts of the document to understand how to comply.
- We are talking about a phased in implementation.
- Putting into applicability section will lock into format and be more confusing.
- Elegance in simplicity but separate document will offer clearer path to receive and interpret comments.
- Do not think we can boil this issue down to key bullets and be comprehensive enough.
- This is too complex to put into the applicability section; compliance and other issues that do not fit in the applicability section. Review as one document now and then disperse into the standards as needed in Phase II; premature to place it in one place or another until we get comments back.
- Believe it is consistent to put in a separate document for implementation.

Following the poll, Scott Mix made some conforming changes in the draft language for "newly identified assets" white paper and presented to the SDT:

- Reviewed the three categories
- Category 3 is not called out directly in the flow chart
- Category 3 is covered by "compliant upon commissioning"
- Auditable Compliant always follows one-year after compliance
- Added storm restoration to the table — unplanned to get service back up for customers
- The dates are linked to quarters

Comments:

- Do we need to add verbiage to explain intent of this section and its applicability?
- The last sentence in adopted proposal frames the question to be asked in the comment form.
- Might include explanation for the time frames used in the table.

- Concerned about how we deal with constructive ambiguity in a large company formed from multiple former companies — each still operates parts of their grid separately.
- If separate delegated authority then should not have to combine and you may not have a single program but need a common governance program
- Three month time frames may not be enough for a large corporation realistically — change all of the 3's to 6's? Or wait for industry comments? Wait for industry comments.
- Can we use "senior management" for consistency?

The SDT then unanimously agreed to move forward this as a separate paper in phase 1.

G. Comment Form

Jeri Domingo Brewer reviewed the SDT sub team's revisions to the comment form based on the revisions to the standards adopted by the team.

SDT Comments on the Comment Form

- No changes have been made by the sub team — following a review comments from NERC.
- Include list of standards and titles in background to be sure industry understands what is being reviewed.
- Editorial changes included deletion of material from the SAR — trying not to confuse industry on what we are doing in phase I, so the sub team is suggesting deleting material that appears to be related to phase II
- Suggest removing the Requirements section that was added by the sub team
- Under Implementation Plan — make clear what the two different implementation plans are trying to do.
- Added to question about what they do not like the request for suggestions to address the concern — may adopt in other standards comment forms too.
- Keep language about intent to educate the industry on what we mean now and in future phases
- Clarify whether the implementation plan only in play during the transition from version 1 to version 2?
- Since we got rid of the second implementation plan, then related language here is no longer needed.
- Footnotes here are helpful in explaining the intent. Check whether the Footnotes work in the new "checkbox" software? May have to use (parenthetical) form.
- Ask Scott Mix and Phillip Huff to come up with questions for the critical asset identification and the effective date respectfully.

The sub-team agreed to review and present a proposal a revised version of the Comment Form before the vote on the Phase 1 package and products. On Friday, Jeri reviewed with the SDT the minor corrections to clarify language on the comment form that included key questions from the Implementation Plan document and from the "newly

identified assets document." The SDT unanimously agreed to adopt the Comment Form at part of the Phase 1 documents.

H. Adoption of Phase 1 Package

On Friday morning, the SDT Phase I package of documents was moved for adoption and submission to the industry for comment (Mover: Kevin Perry, second: Sharon Edwards). The Phase 1 Package was adopted unanimously without discussion.

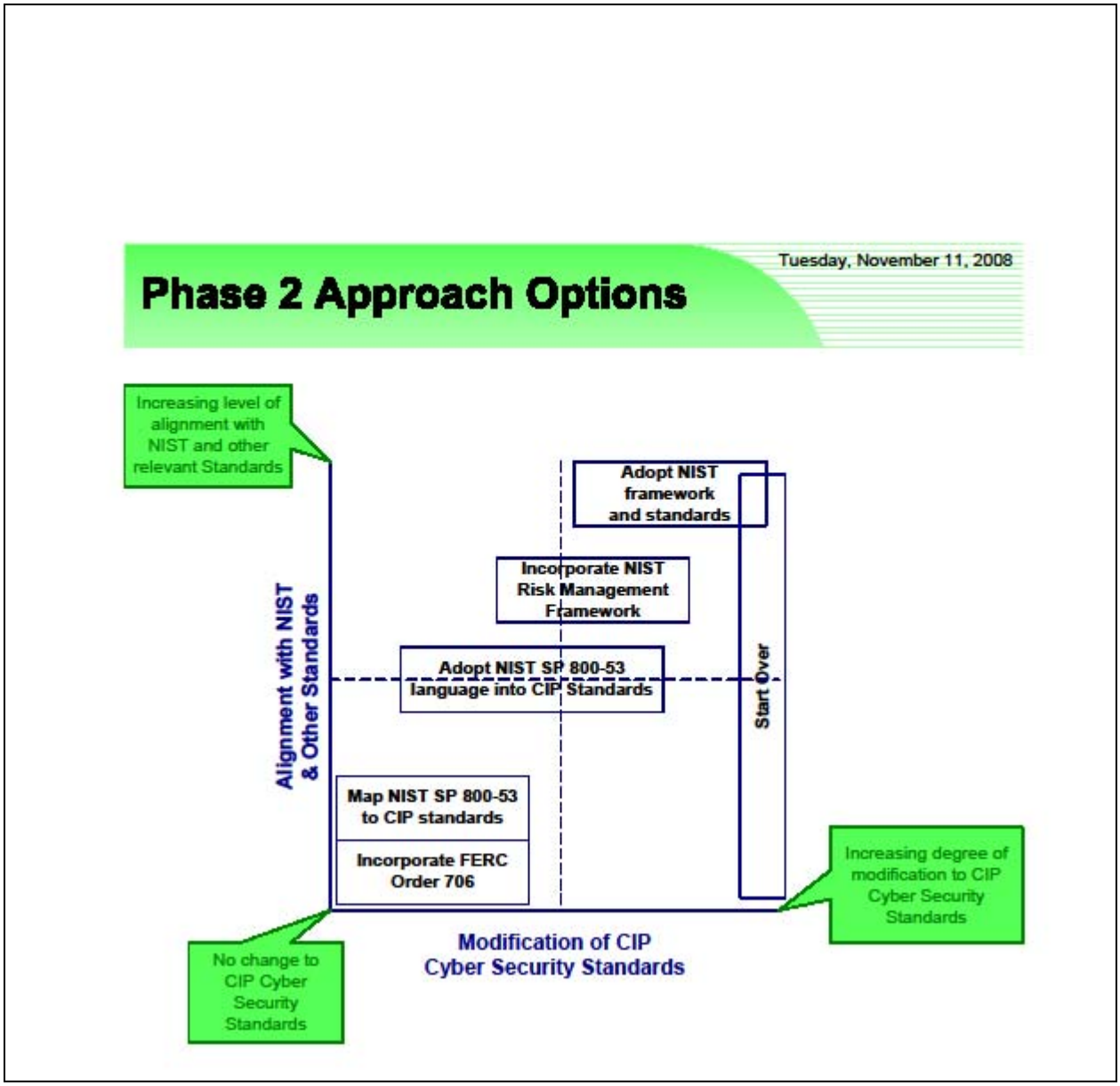
Phase 1 Package of Documents	Adoption Vote	
Phase I Document Motion to Adopt *(Mover, Kevin Perry, Second, Sharon Edwards)*.	21	0

VII. INITIAL REVIEW OF PHASE II APPROACH

A. Review of the Facilitators' Phase II Options Paper

The SDT at its first two meetings discussed how to develop a clear roadmap for how it would engage on the issues and products in Phase II. At the conclusion of the Sacramento meeting, the Chair asked the facilitator to develop an options paper for review at the Little Rock meeting following the adoption of the Phase I package. During an interim WebEx call, the Chair invited any member to send any thoughts on the options to the facilitators. The facilitators received comments and suggestions on approaches and options from John Varnell, Bryan Singer and William Winters and worked closely with the Chair and the Vice Chair in producing the options white paper *(See Appendix # 7)*.

The paper suggested there is a foundational issue concerning the relative merits of the CIP and NIST (and other) cyber security standards that should be addressed for several reasons. One reason is the attention that FERC Order 706 gives to this issue (*See Appendix # 9)*; second it raises questions about the basic paradigm that NERC uses in standards development and oversight; and third, how this matter is addressed by the SDT will influence how it may address many other issues raised in FERC Order 706. For these reasons, the paper suggested the next item on the SDT agenda at the conclusion of submitting the Phase I document will be a review of the CIP cyber security standards in relation to relevant standards developed by NIST and others. A diagram was offered to graphically describe a way to chart the options presented for Phase II.



SDT Initial Comments on the Phase II Options Paper:

- Option E is probably not acceptable under the NERC standards development process.
- We are on risky ground adopting a NIST risk management framework because it allows the entity to accept risk. FERC has stated that is not acceptable.
- NIST has a process for identifying risks that are very difficult to contain and a process to gradually work your way out of that situation. We need to have that discussion with FERC.

- Problem with current standards is that the acceptance of risk was decoupled from risk assessment.
- The FERC order is regulatory law and we cannot decide to ignore and go another direction.
- Missing link: FERC said to look at FISMA/NIST. FIPS 199/200 looks at risk profile. Things are different between the datacenter and the field sites. What is missing is "how much do I really need to worry about this?"
- We have got to do something about the cherry-pick approach to security found in the current standards.
- Need to group of all the issues to best determine the best approach for tackling them. Perhaps putting together multiple spreadsheets and sources of those issues.
- Note there are many suggestions in the SAR for process development aimed at NERC rather than the drafting team.
- For the SDT Scope, are we relying here only SAR 706? Are we only focusing on the FERC 706 order for our decision?
- Our charge is to consider all of the options from doing nothing to complete adoption of the NIST framework — the strawman is to test multiple options for responding to FERC
- The last two options (E and F) mention discarding — that is probably too harsh
- Also not adopting but will be adapting NIST into CIP?
- SAR notes the SDT can and perhaps should reassess everything
- E — Adopting NIST framework — does not meet the NERC process and is not allowed — adapting it may be a severe form of option C.
- F may be where FERC directive asks us to go but keep in mind that the original 15799 was the framework for the 1200 standard the industry started with and long since moved past.
- Has FERC told us the direction but also indicated that the direction is not acceptable — need to manage expectations based on risk assessment directions in the SAR
- Last two options have problems for adopting them in terms of responding to FERC.
- Acceptance of Risk — 706 language developed by lawyers and substance people may not be happy — we have to make it happen practically — process for easing our way out of the problem — FERC may be trying to "have their cake and eat it too"
- This would require a massive funding of a new system — need to practically work toward a more acceptable method of getting out of the problem developed over the past 100 years — FERC can not have it both ways
- Do not assume FERC is adverse to risk acceptance if we can show a practical way of addressing the issue.
- We have no choice to follow what is in the order regarding the CIP standards unless a contravening order is issued — it is the current law.

- Can comment within the law — just setting foundation for addressing additional issues beyond phase I
- Several of the options presented seem to overlap and say some of the same things — need not to bog down in discussing this and need to move on to meatier matters of substance.
- Look to NIST to see if there is anything we can approve — one issue is the residual risk — figure out your risk profile or impact — need levels of gradation of risk as a target — same goes for facilities, some more vulnerable or have a bigger impact — NIST framework helps address these two sets of gradation
- Commend facilitators for capturing the essence of the issue in the options to get us through the discussion to set the framework for dealing with the issues
- Today we "cherry pick" the issues in cyber security with a focus on what should not be covered — we have to figure out how to deal with this under any of the options offered.
- Not identifying new standards but to look at cyber security as it relates to bulk power production, not try to do everything
- We may not have a good concurrence on the scope of what we are being asked to do — the criteria help us focus on what needs to be considered — is there any support for throwing out the system and starting over?

B. Review of Draft Assessment Criteria

The facilitators presented some initial draft assessment criteria (*See Appendix #8)* and invited the SDT to clarify, revise or add additional criteria. The facilitators suggested the criteria could help provide a frame for each member to assess the acceptability of the various options for how to proceed. The criteria also offer an initial opportunity for the SDT to discuss key issues related to how to proceed. The facilitators noted that the mechanics of the proposed review process will include looking at each option to identify the pros/cons of each on its merit *(see Appendix # 8),* then ranking each option for acceptability and ending up with list ranked from top to bottom in terms of acceptability. The SDT could look at lower ranked options and see if anything is worth retaining or incorporating into the most acceptable framework option.

SDT Comments on Draft Criteria

- Suggest decoupling E between implementation and compliance and making this two criteria.
- Are these weighted for relative importance between the criteria? No. Enhancing cyber security should be given a higher weighting
- Goes to how we use these criteria — intended for guiding discussion not a formal formula for scoring each option
- Corollary to D — does the option do the most for advancing the reliability of the bulk power system? That is the object of ensuring cyber security
- Does it protect the investment we have already made in adhering to the CIP standards? — dollars or economic question — builds on what we have already done

- Which option best addresses the foundational issues? Foundational issues includes risk assessment is never done in the current system; also everything such as people and facilities are seen from a box — brainstorm a list of the key foundational issues — something is either critical or not, no gradation
- How does the option identify and mitigate the risk? Option that does the most to identify and mitigates risk.
- Which approach allows to extend into related issues — smart grid with new standards, distribution automation, etc. — from electronic systems view, being able to hack into system versus physical access to a facility — we are the most central system, other systems are looking to us for a model
- Possible criteria: "Does not drive industry to overly secure"
- This is not a one size fits all approach to assessing and securing risk, E.g. the impact on rural farm areas is different than impact on key urban facilities. This requires different assessments and levels of attention.
- Trying to protect bulk power system not the distribution (if not with in the production system)
- Will help if we move FAQs out as guidance to get them the attention they need for clarifying issues.
- Different types of bulk system production requires different levels of protection — vary in types of risk to be addressed
- C in CIP is not "cyber" but "critical" infrastructure protection. Need to stick with cyber security — it is in the Team's title.
- We are looking at the strategy for addressing issues in phase II, not the scope — that was developed by the SAR team, with flexibility for how to address the issues
- Drop off options that are not designed to significantly address issues identified in SAR
- F — double weights other criteria — "If expensive then it would not be supported by ballot,."
- Need to use a risk analysis process — that would help us to focus.
- "Support at ballot" is not a good criteria — no changes at all would be the most supportable at the ballot — need to keep in mind that we are protecting the bulk electric system and the focus is on cyber security
- To move forward there may be too many options and criteria for weighing and judging among them — also some of the answers to the criteria questions may be too subjective.

SECOND DRAFT PHASE II OPTIONS ASSESSMENT CRITERIA
(Not Weighted nor Prioritized)

Initial Draft Criteria as Revised by SDT in November 14 Discussion

D. The option is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
E. The option is achievable given the SDT schedule and work plan.

F. The option does most to advance and enhance cyber security.
L. The option helps the SDT address the foundational issues with the current standards.
M. The option is capable of implementation.
N. The option is capable of improving compliance.

New Criteria Identified by SDT in November 14 Review

O. The option helps protect the current investments and wherever possible builds on what has already been done.
P. The option helps to identify and mitigate risk on an ongoing basis
Q. The option balances a systems orientation with a facilities orientation to asset protection approach. The option is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
R. The option enables the industry provide the appropriate level of security (not over securing nor under securing the cyber assets).
S. The option allows for discrimination among the various types of infrastructure that supports the BES

C. Review and Ranking of Optional Phase II Approaches

The SDT then discussed refining and reducing the number of optional approaches to consider and rank:

SDT Comments on Approaches

- We need to tackle risk assessment first — everything else follows CIP 002 — that will drive the rest of the options — CIP 2 is not cyber security but is risk assessment
- Options: A is a must do, FERC will use as a check list and if not addressed then will shot us down and say start over; but other options may follow question on CIP 2 — look at NIST to see what it says about each issue, NIST stuff is not copyrighted and we can steal as needed
- A, B, C and some of D — the right approach is an amalgam of the options with A as the lead or preliminary discussion
- How much alignment do we have to start with? The groupings can be realigned — are we to fill the worksheet out for the next meeting? Group into three options and see where we fall as group — are we aligned or not — where on the graphic do we fall as a team?
- The question is where to start? The industry is about producing electricity — we are different — is it a facilities oriented framework or a systems oriented framework? - is it a physical asset protection or information system protection? Do we start with NIST framework and ask what is the right thing to do, checking with the 706 spreadsheet of issues? Or do we continue to cherry pick with current standards? Start with NIST mindset or CIP mindset?
- CIP has a huge acceptability in the industry to start with. What percentage of the CIP standards are acceptable to FERC? Offers a head start over the NIST standards.

- Do we need a broader discussion of risk assessment before discussing the framework?
- Is everyone familiar enough with NIST to assess its value as a starting framework?
- Concerned with setting to narrow a solution for guiding the discussion — need to look at the overall risk to be addressed first — previously we found a solution and fit the problem to it
- We need to look at the FERC order — want us to fix the standards, not replace them or start over — identified the things we need to fix — can look to NIST to see if it fixes particular problems
- Question on process — living with CIP standards and only read NIST standards in one day — need to take a deeper dive into NIST before deciding — utilize experience at the table as to how both are applied

The Chair suggested and SDT agreed to "test the team's pulse" by ranking the acceptability of four identified options for going forward and then to design the December agenda around the approach receiving the greatest support from team members. Below are the results of that exercise:

PHASE II WORK PLAN OPTIONS IN RANK ORDER
(As identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**9**	**5**	**4**	**0**	**3.27 of 4**

2. Adopt/adapt NIST into CIP or Merge NIST into CIP

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**3**	**9**	**4**	**0**	**2.93 of 4**

3. Revise CIP as directed — leave as is and add in only items identified by FERC order

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**5**	**7**	**7**	**0**	**2.89 of 4**

4. Start Over — in terms of a starting point

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
11-14 rank	**2**	**5**	**7**	**5**	**2.21 of 4**

The Chair agreed to plan for the December agenda with this in mind.

VIII. TECHNICAL FEASIBILITY

Scott Mix reviewed the "Technical Feasibility" eight page document with two pages included of questions which were reviewed at the Sacramento meeting. This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round to send to the SDT for review prior to December. He noted the goal would be to post a paper approved by the team for comment soon after the December meeting. The comment period would overlap with the Phase I period but would last longer.

SDT Comments on Technical Feasibility

- Purpose is because "reasonable business" not stricken yet and this is set for audits after June 1

IX. NEXT STEPS AND EVALUATION

A. NERC Phase One Communication Plan

The Chair asked whether NERC was developing a communication strategy for supporting this project. Dave Taylor noted he was still working with Gerry Adamski to develop the strategy and that they hope to have something ready to present at the December meeting. The Chair noted she prefers to have a session with the industry as soon after posting the package as possible to ensure they have the information they need before commenting. Mr. Taylor agreed to have a NERC presentation on the plan at the December SDT meeting.

B. Review of Phase I Schedule

Dave Taylor reviewed the potential schedule to complete the Phase I process by the end of June 2009. He noted the concerns that times are tight but noted the schedule provides very limited flexibility to extend the comment time — if we do so it extends the end of the time line into the middle of July.

SDT Comments:

- Changing the time frame will not help much — extending the time will not change how people vote.
- Important from a perception point to get this in on time to FERC — getting in after date may show too little concern for their directives— NERC and industry are under the gun.
- To do a realistic quality job and seriously respond to comments the schedule proposed gives us a defensible position that this is complicated and needs more than eighteen months — The Phase I experience will show FERC why it takes more time.
- Is this the fast track process promised by NERC CEO or is this the same process trying to go faster? No, this is not the fast track process.
- Holidays leaves people the first weeks of December to comment and we will offer WebEx explanation after first week? The comment period ends in early January just before the scheduled Phoenix SDT meeting.
- Credibility with FERC is important — need to meet the deadline is important
- Need to do the best we can to get the message out and input back but within the time deadline — set a conference call to discuss the communication plan
- Schedule offered, with three comment periods, Phase II ends April 2011 — draft subject to discussion to follow on proposals for concept approach to Phase II

C. December Meeting Agenda Review

NERC announced that the next meeting will take place in law office in downtown Washington, D.C. downtown and will be a two day format from 8 a.m.–5 p.m. on day one and from 8 a.m.–3 p.m. on day two to allow for travel out on a Friday.

The proposed agenda items include:

- Review elements of communication plan for Phase I,
- Technical Feasibility review,
- Background on NIST and its application, and

- Continue discussion of Phase II approach.

D. SDT Meeting Evaluation — What Worked and What Could Be Improved?
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?

- AECC is a GREAT meeting facility (Thanks to Phillip)
- Quick polls
- Attitude of the group as a whole very good and productive
- Like idea of breaking into sub-teams for editing documents
- Best meeting so far to participate in by WebEx
- Learned from SDT mis-direction and bounced back
- Came up with an edit rejection method for use while editing text
- Building arsenal of processes and when to use them
- Several team members stepped up and did a lot of extra effort
- Rich distinguished between "its" and "the" — the devil is in the detail and haste makes waste
- Everyone is not bashful about speaking up
- Devil is in the details — got to get it right — avoided temptation to rush to quickly past the details that make a huge impact.

What could be improved?

- Need a UBS for meeting rooms in the future
- Take opportunity to take straw polls sooner to keep us moving
- Bogged down
- Veered from time table
- Confusion over consensus procedures and use of parliamentary procedures and Robert's Rules
- Need tighter oversight from the facilitators. Facilitators could help us more avoid unintended discussions and detours
- Did not get a draft of the Communications Plan from NERC in advance as promised
- Need to have drafts available before meetings
- WebEx master needs to have all documents ahead of time

Other Comments

- Assumed NERC review would be tech-writing format only
- Need pre-review opportunity for NERC edited documents
- Frustration over the process but it is a good thing to realize decisions are hard but need to deal with issue
- Did not get a draft of communications plan as promised
- Making sure long edits are available prior to the meeting
- Help if WebEx has documents ahead of time

- Pre agreement for the process to deal with documents is helpful
- Gap in process — assumed NERC review would be a limited review — turned out to be much more extensive — would have been helpful to have an opportunity to review ahead of time — lack of opportunity to see and address ahead of time
- Appreciate the efforts of Scott and Jackie and others who committed extra time to help us move forward
- Sub teams stepped up and efforts were appreciated
- Important for everyone to speak up and we need to stop and pay attention when needed
- What matters are the words that make it onto the paper not just what we think they mean — others outside the room will read without the underlying discussion — need words to accurately communicate what we mean
- Thank you to Phillip again for hosting

Members agreed to adjourn at 11:30 a.m. on Friday until the next meeting on December 4–5, 2008 in Washington D.C.

Appendix # 1
Meeting Agenda
Cyber Security Order 706 SDT — Project 2008-06

November 12, 2008 — 1–5 p.m. EST
November 13, 2008 — 8 a.m.–5 p.m. EST
November 14, 2008 — 8 a.m.–noon EST
Little Rock, AK

Wednesday	**November 12, 2008**
1:00 p.m.	Welcome and Opening Remarks- Jeri Domingo-Brewer and Kevin Perry
1:05	Roll Call — Harry Tom
1:10	Review NERC Antitrust Compliance Guidelines — Harry Tom
1:15	Adopt October 22 Meeting Summary and Review of Meeting Objectives — Bob Jones
1:20	Organizational Issues — Stuart Langton ▪ Review of Work-plan ▪ Adopting the SRT Consensus Guidelines ▪ SRT Purpose Statement
2:00	Phase I Products Review and Refinement
3:00	Break
3:15	Phase I Products- Review and Refinement
5:00	Observer Comments and Suggestions
5:15	Summary of Day One Outcomes and Review of Day Two Agenda
5:30	Recess
Thursday November 13, 2008	
8:00	Welcome and Agenda Review
8:10	Phase I Products — Refinements and Straw Polls
10:00	Break
10:15	Phase I Produces — Refinements and Straw Polls
12:00	Working Lunch
1:00	Phase I Products — Refinements and Straw Polls
3:00	Break
3:15	Phase I Products Refinements and Straw Polls
5:00	Adoption of Phase I Products
5:15	Summary of Day Two Outcomes and Review of Day Three Agenda
5:30	Recess
Friday November 14, 2008	
8:00	Welcome and Agenda Review
8:10	Phase II Work-plan Review and Discussion — Review of Concept(s) Submitted and Straw-man
9:00	Phase II Discussion of Foundational Assumptions, Approach and Expectations
10:00	Break
10:15	Phase II Ranking and Discussion of Optional Approaches
11:30	Assignments, Next Steps, and Review of Work plan
12:00	Adjourn

Appendix # 2

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

Little Rock, Arkansas
November 12–14, 2008

Attending in Person — Team Members

1 **Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
2. Jackie Collett	Manitoba Hydro
3. Jay S. Cribb	Information Security Analyst, Principal, Southern Company Services, Inc.
4. Sharon Edwards	Project Manager, Duke Energy
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp.
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
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 Corporation
11. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
12. David S. Revill	Georgia Transmission Corporation
13. Scott Rosenberger	Luminant Energy
14. Kevin Sherlin	Sacramento Municipal Utility District
15. Michael Winters	Arizona Public Service Co.
1. David Taylor	NERC
2. Harry Tom	NERC
4. Scott R. Mix	NERC
5. Todd Thompson	NERC
6. Hal Beardall	FSU/FCRC Consensus Center (November 13 & 14)
7. Robert Jones	
8. Stuart Langton	FSU/FCRC Consensus Center

SDT Team Members Attending via WebEx/Phone

1. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co.
2. Tom Hoffstetter	Midwest ISO, Inc *(November 13 and 14 only)*
3. Christopher A. Peters	ICF International *(November 12 and 14 only)*
4. Jonathan Stanford	Bonneville Power Administration
5. John D. Varnell	Technology Director, Tenaska Power Services Co.
6. William Winters	Hydro One Networks, Inc.

SDT Team Members Unable to Attend or Participate by WebEx

1. Bryan L. Singer	Kenexis
2. Keith Stouffer	National Institute of Standards & Technology

Attending in Person — Participants

1. John McGlynn	PJM
2.	Arkansas?

Attending via WebEx — Participants

6. Matt Schnell	Nebraska Public Power District
7. 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 Phase I Products

Below is a link to all of the documents reviewed by the SDT including final Phase I products with both clean and red-lined versions agreed to during the full Team discussions in Little Rock:

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix # 5 SDT Consensus Guidelines

Adopted Unanimously, November 13, 2008

Cyber Security for Order 706 Standard Drafting Team

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.

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

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

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

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

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

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 and 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** (use of name tents to seek attention)

- **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 and as a poll to see where the Team stands, not used as a voting mechanism.
  - 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

- **Consensus Ranking Scale**
  4. Comfortable — I support proposal as is ♥♥♥♥
  3. Minor Reservations — I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your

concerns.

2. Major Reservations — I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
1. Fatal Flaws — I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

- **Robert's Rules of Order and Facilitated Consensus Building Procedures**
  The Council will make substantive recommendations using their adopted facilitated consensus-building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

Appendix # 6
Day One NERC Edit Review

CIP-002 November 13	# of Members Not Accepting NERC Edits (6 o more= reject edit)	Accept/Reject
Introduction A.3 Purpose Edits	**20** (16/4 ph)	Reject
A.4 Regional Entit~~ies~~y	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept
R1 Edits	**7** (5/2 ph)	Reject
R1-4 Edits - Delete Titles	**6** (5/1 ph)	Reject
R2 Edits	**10** (8/2 ph)	Reject
R3 Edits, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R3 Edits- delete examples	**2** (2/0 ph)	Accept
R3 other edits	**12** (12/0 ph)	Reject
R4 Edits- including deletions and footnote	**10** (8/2 ph)	Reject
R4 Delegate~~'s~~ Delete 's	**2** (2/0 ph)	Accept
C. Measures - Delete preamble/intro	**2** (1/1 ph)	Accept
M1 Edits	**2** (2/0 ph)	Accept
M2 Edits	**2** (2/0 ph)	Accept
M3 Edits	**1** (1/0 ph)	Accept
M4 Edits including delete "of annual"	**1** (0/1 ph)	Accept
D. Compliance		
1.1-1.3 Edits *Global to all CIP requirements*	**0 (**0/0)	Accept
1.4.1 Edits	**0 (**0/0)	Accept
1.4.2 Edits	**14(**13/1 ph)	Reject
1.5.1 Edits *Global to all CIP requirements*	**0 (**0/0 ph)	Accept
D.2. Delete/add "violation severity levels"	**1** (1/0 ph)	Accept
Version History- NERC to revise consistent with changes above		Accept

CIP-003 November 13	# of Members Not Accepting NERC Edits (6 or more= reject edit)	Accept/Reject
Introduction A.3 Purpose Edits GLOBAL	**20** (16/4 ph)	Reject
A.4 Regional Entit~~ies~~y GLOBAL	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept
R1, Delete "Identifies" add "represents"	**7** (7/0 ph)	Reject
R1-6 Edits- Delete Titles	**6** (5/1 ph)	Reject
R3 Edits,	**10** (10/0 ph)	Reject
R3.1	**7** (7/0 ph)	Reject
R3.2	**7** (7/0 ph)	Reject
R3.3	**8** (8/0 ph)	Reject
R4 Edits	**20** (16/4 ph)	Reject
CIP- 003	# of Members Not Accepting NERC Edits (6 or more= reject edit)	Accept/Reject

R4 Edit, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R5 Edits, delete ~~the~~, substitute its	**2** (2/0 ph)	Accept
R5.1	**2** (2/0 ph)	Accept
R5.1.1	**0** (0/0 ph)	Accept
R51.2	**0** (0/0 ph)	Accept
R5.3 Edit, delete ~~the~~, substitute its	**0**(0/0 ph)	Accept
C. Measures- Delete preamble/intro	**2** (1/1 ph)	Accept
M1-6 Edits	**1** (1/0 ph)	Accept
M4 Edits including delete "of annual"	**1** (0/1 ph)	Accept
D. Compliance		
1.1-1.3 Edits *Global to all CIP requirements*	**0 (**0/0)	Accept
1.4.1 Edits	**0 (**0/0)	Accept
1.4.2 Edits	**14(**13/1 ph)	Reject
D.2. Delete/add "violation severity levels"	**1** (1/0 ph)	Accept
Version History- NERC to revise consistent with changes above		Accept

CIP-006	***# of Members Not Accepting NERC Edits*** *(6 or more= reject edit)*	***Accept/Reject***
Introduction A.3 Purpose Edits GLOBAL	**20** (16/4 ph)	Reject
A.4 Regional Entiti~~esy~~ GLOBAL	**20** (16/4 ph)	Reject but make "Entity"
B. Requirements Delete Preamble	**1** (1/0 ph)	Accept

TABLED, November 13

Appendix #7
Options Paper—Phase II

OPTIONS FOR REVISING THE CIP CYBER SECURITY STANDARD(S)

As the SDT completes its phase I work, it needs to determine what issues it will next address and in what order. However, prior to so doing, there is a foundational issue concerning the relative merits of the CIP and NIST (and other) cyber security standards that should be addressed for several reasons. One reason is the attention that FERC Order 706 gives to this issue; second it raises questions about the basic paradigm that NERC uses in standards development and oversight; and third, how this matter is addressed by the SDT will influence how it may address many other issues raised in FERC Order 706. For these reasons, it is proposed that the next item on the SDT agenda at the conclusion of submitting the Phase I document will be a review of the CIP cyber security standards in relation to relevant standards developed by NIST and others.

Among the points that FERC makes regarding the NERC Cyber Security Standards and those developed by NIST and others, the following seem particularly relevant for the SDT to consider:

1. FERC "believes" that NIST standards "may" provide valuable guidance in developing "future" iterations of CIP standards (sec. 25).
2. FERC "directs" NERC to review revisions in the CIP standards "considering applicable features of the NIST framework." (sec. 25).
3. FERC states it will not delay the "effectiveness" of CIP standards by "directing replacement" of the CIP standards "with others based on the NIST framework." (sec. 25)
4. FERC says it, "will not at this time direct NERC to incorporate specific provisions of the NIST standards," and adds, "that immediate adoption of the NIST standards would result in unacceptable delays (sec.232).
5. FERC says it "believes" NERC "should monitor" the development of NIST standards to see if they contain provisions that may be better than the CIP standards (sec.233).
6. FERC "directs" NERC to "consult with federal agencies" that use both CIP and NIST standards regarding effectiveness and implementation issues concerning NIST and to, "report these findings to the Commission.," (sec. 233).
7. FERC says it "may" revisit this issue in future proceedings as part of their evaluation and assessment of NERC (sec. 233).

Given the above comments, and others from FERC, the NERC Standards Committee has included the following in its directions to the SDT.

"Revisions should consider other Cyber-related standards, guidelines and activities:

- Consider adopting the NIST Security Risk Management Framework (includes GAO, OMB and FIPS)
- Consider other cyber security related documents such as NIST, ISO 27000 Family,
- CIPC WG Risk Assessment Guideline, MITRE Corporation technical report, DHS,

- National Laboratoires papers, DOE 417, IEC, ISA, etc.
- Stay apprised of coordination work between FERC, NEI and NRC in regard to the nuclear facility exemption issue with respect to regulatory gaps. As necessary modify the standards to reflect current determinations."

FERC Order 706 and the directions provided by the NERC Standards Committee suggest a degree of latitude for the SDT in what they may conclude regarding consideration of the NIST Security Risk Management Framework, applicable features, or elements of other security related documents. In regard to the challenge this presents to the SDT, several members have offered suggestions. John Varnell, for example, points out the compatibility of CIP and NIST standards and suggests, "each CIP requirement can be mapped to a NIST 800-53 requirement." This is consistent with the NIST briefings the SDT was given at its first meeting. John goes on to suggest that the SDT develop a guide that will show how NIST requirements can comply with each CIP requirement. Bryan Singer supports this and suggests other relevant standards need to be considered and that attention needs to be given to whether any optional standards meet the intent of a compliance requirement. William Winters suggests that the SDT should first identify its foundational assumptions, of which he offers some examples and alternatives such as: "…adopt the NIST framework and proceed with a roadmap on that basis," "The team should dump the whole standard and start over," and ,"read each FERC concern and adjust current standard as little as necessary to address the concerns."

In keeping with the above suggestions, it is proposed that the SDT consider six options, which, as Phase II Approach Options graphic and the list below illustrate, range from more modest to more sweeping alternatives:

A. Incorporate FERC Order 706. Modify the CIP standards to incorporate the requirements of FERC Order 706. Modify the CIP standards as necessary to address the other requirements of the SAR. Evaluate splitting industrial control systems (ICS) into own set of standards.

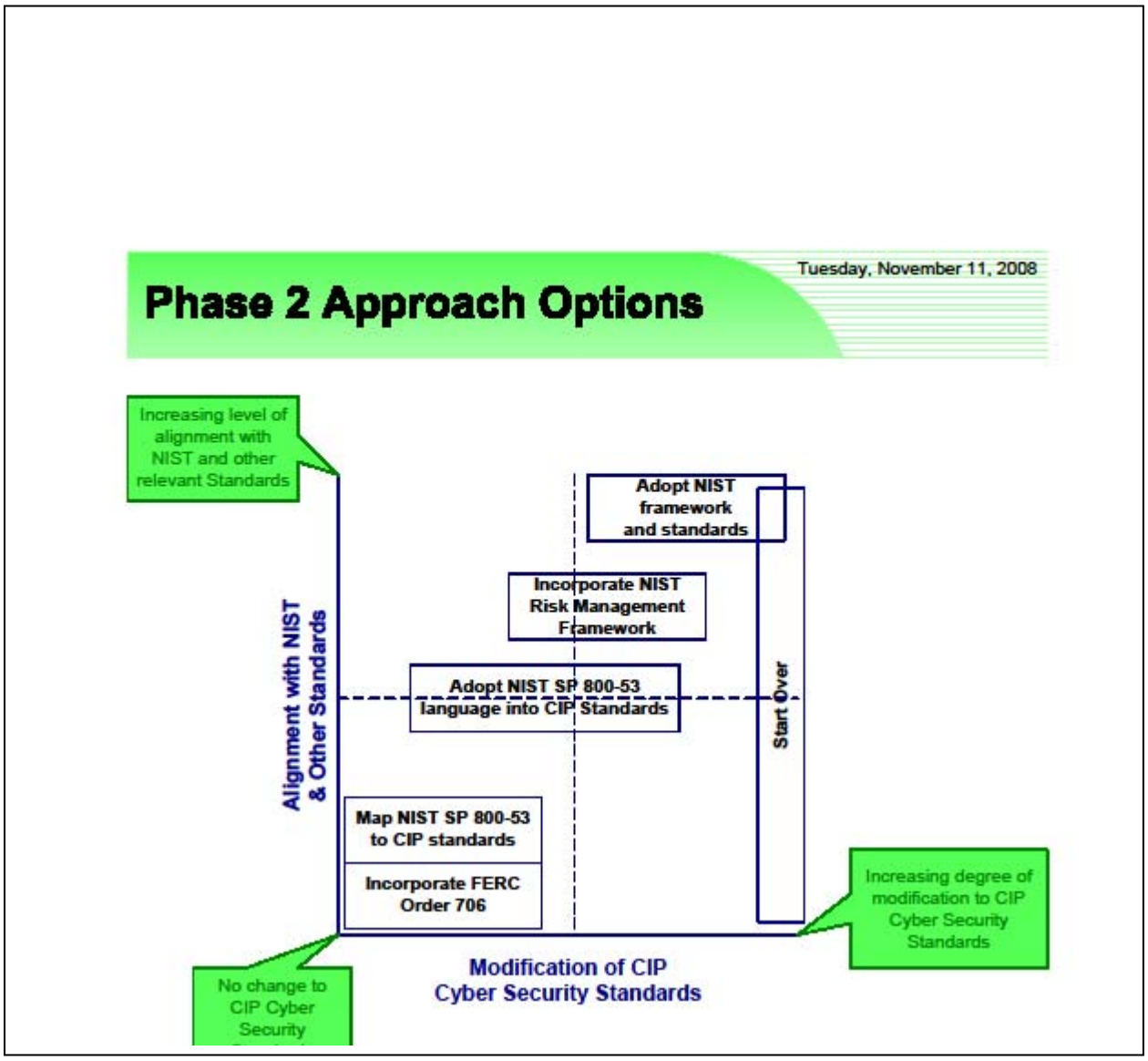
B. Map NIST SP 800-53 to CIP standards: Map similarities and differences between the CIP standards and NIST 800-53 requirements, and provide guidance as to how they can be managed separately but in concert with each other.

C. Adopt NIST SP 800-53 language into CIP standards. In addition to incorporating Option A, provide specific mapping between the CIP standards and the requirements of NIST SP 800-53. Evaluate and modify the language of CIP standards requirements and measures in light of NIST SP 800-53.

D. Incorporate NIST Risk Management Framework. In addition to incorporating options A and C, evaluate and incorporate the NIST Risk Management Framework into the CIP standards. This would predominately impact Critical Cyber Asset identification and technical feasibility/risk mitigation.

E. Adopt NIST framework and standards: Replace CIP Standards with NIST Risk Management Framework and SP 800-53/SP 800-82. This approach represents the wholesale adoption of the NIST framework and discards the existing CIP standards.

F. Start over. Evaluate all available security/risk management frameworks, including ISO



17799/27001, ISA 99, and NIST/FISMA. Select a framework and adopt it fully in place of the existing CIP standards.

It is proposed that the SDT assess these options, identify others that may be as appropriate, and consider modifications or combinations of them. To do this, it may be helpful for the SDT to select assessment criteria, identify the pros and cons of each option, and to rate the various options in regard to levels of acceptability.

Appendix #8 — Phase II Options Review Worksheet

This worksheet was developed by the Facilitators for use on November 14 to guide the STD discussion on approaches and options to Phase II on November 14

SDT PURPOSE STATEMENT

CYBER SECURITY FOR ORDER 706 STANARD DRAFTING TEAM
(adopted unanimously by the SDT, November 13)

The Cyber Security Order 706 Standards Drafting Team (SDT) is serving in the public interest throughout North America to protect the critical cyber assets (including hardware, software, data, and communications networks) essential to the reliable operations of the bulk power system.

The overall purpose of the SDT is to work together to build consensus on a technically sound and complete package of recommended cyber security standards and a realistic implementation plan that is responsive to and consistent with the scope of the Standard Authorization Request (SAR), the FERC Order 706 and the ANSI process.

DRAFT STRAWMAN OPTIONS ASSESSMENT CRITERIA

Review the draft strawman assessment criteria below. If you have an additional criterion you would like to propose, we will solicit those. We will rank, discuss and refine all proposed criteria. Members can utilize these criteria in the evaluation and assessment of each of the Phase II Options:

A. **The option most parallels the SDT purpose statement**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

B. **The option is responsive to the FERC 706 directives and the SAR.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

C. **The option is achievable in time-- in terms of the SDT developing the proposed standards.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

D. **The option does most to advance and enhance cyber security**

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

		reservations	*reservations addressed*	
11-14 initial rank				

E. **Most capable of implementation.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

F. **Most capable of compliance.**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

G. **Is most supportable by ballot**

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

DRAFT STRAWMAN OPTIONS

INSTRUCTIONS: Take a minute to list pros and cons for each of the 6 options. We will review and discuss these. Then we will ask you to rank each on its own keeping in mind the assessment criteria. We will then present these in order of rank (highest average ranking score) and see if there are ways to include pros of other options not selected.

A. Incorporate FERC Order 706.

Modify the CIP standards to incorporate the requirements of FERC Order 706. Modify the CIP standards as necessary to address the other requirements of the SAR. Evaluate splitting industrial control systems (ICS) into own set of standards.

+++++ Pros- Strengths +++++	**------- Cons- Weaknesses --------**
•	•
•	•
•	•

Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

B. Map NIST SP 800-53 to CIP standards:

Map similarities and differences between the CIP standards and NIST 800-53 requirements, and provide guidance as to how they can be managed separately but in concert with each other.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

C. Adopt NIST SP 800-53 language into CIP standards.

In addition to incorporating Option A, provide specific mapping between the CIP standards and the requirements of NIST SP 800-53. Evaluate and modify the language of CIP standards requirements and measures in light of NIST SP 800-53.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

D. Incorporate NIST Risk Management Framework.

In addition to incorporating options A and C, evaluate and incorporate the NIST Risk Management Framework into the CIP standards. This would predominately impact Critical Cyber Asset identification and technical feasibility/risk mitigation.

+++++ Pros- Strengths +++++			------- Cons- Weaknesses --------	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial				

rank				

E. Adopt IST framework and standards:
Replace CIP Standards with NIST Risk Management Framework and SP 800-53/SP 800-82. This approach represents the wholesale adoption of the NIST framework and discards the existing CIP standards.

+++++ Pros- Strengths +++++			**------- Cons- Weaknesses --------**	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

F. Start over.
Evaluate all available security/risk management frameworks, including ISO 17799/27001, ISA 99, and NIST/FISMA. Select a framework and adopt it fully in place of the existing CIP standards.

+++++ Pros- Strengths +++++			**------- Cons- Weaknesses --------**	
• • •			• • •	
Acceptability Ranking Scale	***4** = acceptable, I agree*	***3** = acceptable, I agree with minor reservations*	***2** = not acceptable unless major reservations addressed*	***1** = not acceptable*
11-14 initial rank				

Appendix # 9 — FERC 706 Background References

Regarding NIST:

25. The Commission believes that the NIST standards may provide valuable guidance when NERC develops future iterations of the CIP Reliability Standards. Thus, as discussed below, we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework. However, in response to Applied Control Solutions, we will not delay the effectiveness of the CIP Reliability Standards by directing the replacement of the current CIP Reliability Standards with others based on the NIST framework.

232. As proposed in the CIP NOPR, the Commission will not at this time direct NERC to incorporate specific provisions of the NIST standards into the CIP Reliability Standards. While commenters provide compelling information that suggests that the NIST standards may provide superior measures for cyber security protection, the Commission is concerned that the immediate adoption of the NIST standards would result in unacceptable delays in having any mandatory and enforceable Reliability Standards that relate to cyber security.

233. The Commission continues to believe — and is further persuaded by the comments — that NERC should monitor the development and implementation of the NIST standards to determine if they contain provisions that will protect the Bulk-Power System better than the CIP Reliability Standards. Moreover, we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission. Consistent with the CIP NOPR, any provisions that will better protect the Bulk-Power System should be addressed in NERC's Reliability Standards development process. The Commission may revisit this issue in future proceedings as part of an evaluation of existing Reliability Standards or the need for new CIP Reliability Standards, or as part of an assessment of NERC's performance of its responsibilities as the ERO.

Regarding an additional guidance/reference document

61. The Commission received comments on both sides of the issue of specificity. Some commenters caution against the CIP Reliability Standards being too specific, while others request more guidance to help them comply. In general, the Commission believes it is appropriate to provide sufficient guidance to explain Requirements so that responsible entities have a high degree of certainty that they understand what is necessary to comply with a Requirement. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. The Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by-case basis. Therefore, in several instances throughout this Final Rule, the Commission gives the ERO direction to provide additional guidance. In some cases, we require

that the guidance be placed in modifications to the CIP Reliability Standards. In other cases, we note that some or all of the additional guidance could be placed in a reference document separate from the CIP Reliability Standards.

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

355. The Commission believes that responsible entities would benefit from additional guidance regarding the topics and processes to address in the cyber security policy required pursuant to CIP-003-1. While commenters support the need for guidance, many are concerned about providing such guidance through a modification of the Reliability Standard. We are persuaded by these commenters. Accordingly, the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address. However, we will not dictate the form of such guidance. For example, the ERO could develop a guidance document or white paper that would be referenced in the Reliability Standard. On the other hand, if it is determined in the course of the Reliability Standards development process that specific guidance is important enough to be incorporated directly into a Requirement, this option is not foreclosed. The entities remain responsible, however, to comply with the cyber security policy pursuant to CIP-003-1.

356. In response to ISO/RTO Council, Ontario Power and other commenters, the Commission's intent in the CIP NOPR — as well as the Final Rule — is not to expand the scope of the CIP Reliability Standards. Requirement R1 of CIP-003-1 requires a responsible entity to document and implement a cyber security policy "that represents management's commitment and ability to secure its Critical Cyber Assets." The Requirement then states that the policy, "at a minimum," must address the Requirements in CIP-002-1 through CIP-009-1. The Commission believes that there are other topics, besides those addressed in the Requirements of the CIP reliability Standards, which are relevant to securing critical cyber assets. The Commission identified examples of such topics in the CIP NOPR. Thus, the Commission, in directing the ERO to develop guidance on additional topics relevant to securing critical cyber assets, is not expanding the scope of the CIP Reliability Standards.

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and

effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document.

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability

assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

575. In response to commenters' questions regarding specific physical access controls, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant physical security. While the Commission continues to believe that a responsible entity must implement two or more distinct and complimentary physical access controls at a physical access point of the perimeter, the specific requirements should be developed in the Reliability Standards development process when the ERO develops its modifications in response to this Final Rule. The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

609 . The Commission has discussed issues related to testing environments in CIP-005-1. In that context, the Commission clarifies the CIP NOPR proposal to require differences between the test environment and the production system to be documented. As stated with respect to CIP-005-1, the Commission understands that test systems do not need to exactly match or mirror the production system in order to provide useful test results. However, to perform active testing, the responsible entities should be required at a minimum to create a "representative system" — one that includes the essential equipment and adequately represents the functioning of the production system. We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1 accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.

621. While we agree that no safeguard will protect against all malicious or unintentional acts, this does not mean that systems should not be protected against such acts. In response to MidAmerican, the Commission believes that details regarding how to safeguard systems against personnel introducing, maliciously or unintentionally, viruses or malicious software to a cyber asset are best developed in the Reliability Standards development process. The revised Reliability Standard does not need to prescribe a single method for protecting against the introduction of viruses or malicious software to a cyber asset by personnel. However, how a responsible entity does this should be detailed in its cyber security policy so that it can be audited for compliance with the Reliability Standard. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes how an entity should protect against personnel introducing viruses or malicious software to a cyber asset. The ERO could also provide additional guidance in a reference document.

629. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The

Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

644. For the reasons discussed in CIP-005-1, in directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the Commission will allow a manual review of a sampling of log entries or sorted or filtered logs. The Commission recognizes that how a responsible entity determines what sample to review may not be the same for all locations. Therefore, the revised Reliability Standard does not need to prescribe a single method for producing the log sampling. However, how a responsible entity performs this sample review should be detailed in its cyber security policy so that it can be audited to determine compliance with the Reliability Standards. The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document. The final review process, however, must be rigorous enough to enable the entity to detect intrusions by attackers.

660. The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. In developing the guidance, the ERO should consider the specific examples provided by commenters, described above. However, we direct the ERO to develop and provide guidance on the term reportable incident. The Commission is not opposed to the suggestion that the ERO create a reference document containing the reporting criteria and thresholds and requiring responsible entities to comply with the reference document in the revised Reliability Standard CIP-008-1, but will allow the ERO to determine the best method to accomplish the goal of better defining reportable incident.

725. The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years. Consistent with our goals and discussion of CIP-005-1, the Commission will not at this time require responsible entities to perform full operational exercises. Instead, the Reliability Standard should require the demonstrated recovery of critical cyber assets in a test environment, with the requirements for representative test environments and for addressing differences between the test environment and the production environment, similar to the conditions discussed for live testing in CIP-005-1. Given the range of views presented in comments regarding live testing, as the Reliability Standard development process forms the details of this “demonstrated recovery”

concept, it should consider offering guidance beyond the actual Requirements of the Reliability Standard in separate reference documents. The Commission believes this alleviates commenters' concerns about the risks associated with such testing