NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

January 7, 2009 | 1–5 p.m. MST
January 8, 2009 | 8 a.m.–5 p.m. MST
January 9, 2009 | 8 a.m.–5 p.m. MST
Phoenix, Arizona, Arizona Public Service

Provisionally Adopted, February 4, 2009 Finally Adopted as Revised, February 19

SDT Meeting Summary by:

Joe Bucciero, Hal Beardall, Robert Jones, and Stuart Langton

SDT Facilitators
Bucciero Associates,
FCRC Consensus Center, Florida State University

Thanks to Team member Tom Hoffstetter for sharing his meeting notes.

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 Standard Drafting Team
5th Meeting Summary
Phoenix AZ

Meeting Summary Contents

EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and a roll call of members and participants in the room and on the conference call was conducted, following review of the proposed meeting agenda. David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines. The SDT agreed to review, and unanimously adopted, the December 4–5, 2008 SDT meeting summary on Friday.

Scott Mix provided an update on the Technical Feasibility Exception process since the SDT December meeting. The Technical Feasibility Exception (TFE) process is based on discussion with utility management. The process is not about the technical requirements and standards that the SDT is addressing, but it is more about whether compliance has been met; compliance is more than just the audit process. Technical feasibility exception was intended to address the issues where compliance could not be met quickly, thereby allowing for good reason to be technically out of compliance while significant issues can be addressed.

The TFE White Paper is being reviewed by NERC management. Compliance and Legal counsel were sought concerning how the white paper should be positioned and what it would mean to enforcement. It needs its own vetting process within NERC, and it may require modification to the Compliance Monitoring and Evaluation Program (CMEP). Changes to the CMEP are applicable across all of NERC's standards, so the TFE needs to well thought through and vetted within NERC. Mike Assante, Chief Security Officer at NERC, has agreed to sponsor the TFE through the compliance process at NERC. Scott Mix will work with NERC Management to determine the best approach for getting this done.

For the Phase I industry comments, Kevin Perry provided a preliminary overview of the 119 pages of comments received from the 46 industry respondents. The comments were organized by NERC staff, and the latest set of comments was released to the SDT on January 7th.

The SDT reviewed several approaches to responding to the Phase I Comments on the cyber security standards. The preferred approach was to break up into small working groups to review an assigned grouping of standards in parallel. There was agreement to begin the Phase II discussion with the full SDT following the development and agreement on responses to Phase I comments. Following the small group breakouts, the full group would meet to discuss the findings and responses from each of the small working groups. Any cross-references or duplicative responses would be addressed and made consistent during this group review session.

Six small working groups were formed to review the industry comments and to develop the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP Standards. The six groups and the SDT members participating included:

Working Group Assignments

CIP Standard No.	Questions Nos.	Assignments/Volunteers
002 & 003	Q1 & Q2	Jeri Brewer, Gerald Freese, Dave Norton, Dave Revill
004 & 007	Q3 & Q6	Chris Peters, Keith Stouffer, Mike Winters, William Winters
005 & 006	Q4 & Q5	John Varnell, John Lim, Rich Kinas, Scott Fixmer, Scott Rosenberger
008 & 009	Q7 & Q8	Tom Hofstetter, Joe Doetzel, Kevin Sherlin
Compliance	ALL Qs	Roger Lampila, Todd Thompson, Jackie Collett
Implementation	Q9, Q10, Q11, Q12	Kevin Perry, Scott Mix, Phil Huff
Q13	Q13	Tom Hofstetter and various small groups

The SDT agreed that whatever was not completed by the end of this meeting (January 7–9, 2009) could be taken up in the WebEx calls scheduled for January 15th and January 21st.

The members of each small working group considered the following in presenting their findings to the full group:

- Present substantive issues and responses from most to least contentious (10–15 total minutes for each small group report);
- The full SDT will focus on most contentious issues to confirm response(s); and
- Small groups may reconvene to refine responses.

The SDT reviewed all 13 questions and draft responses to industry comments and addressed compliance issues raised across all of the comments.

On the third day the small groups met again to review and refine their comments further in light of the SDT review on day two.

Scott Mix introduced John Sykes, Vice Chair of the NERC System Protection and Control Subcommittee, which is looking at redundancy in control and protection systems, as an aspect of critical asset protection. They are early in their process of review. The NERC SPCS has written a technical white paper, a proposed working paper for a standard, and has prepared the

presentation. It took two an a half years to get to this point, and the SPCS need lots of industry input because of the high potential cost to the industry. The major topic of discussion was on the methods for determining risk. Do we write a prescriptive standard or a performance-based standard? Key initial question, helped decide on the performance based approach.

Stu Langton introduced a review of the Phase II White Paper process. He reviewed discussion from the previous SDT meeting in Washington where we came away with proposal to prepare and review two straw proposals, one starting from the CIP standards perspective and looking to incorporate applicable NIST concepts and the other starting from the NIST standards perspective and looking to incorporate CIP concepts.

Jackie Collett took a look at the NIST 800-53 standard and sees promise, but she also sees aspects of the standard that may cause concern for electric power systems. Jackie reviewed her take on the original intent of the NERC CIP-002 standard. William Winters offered initial thoughts on his approach from NIST, and how he might address some of the gaps in the standards but recognizing the concerns the industry may have with the NIST risk assessment approach, particularly cost. Bill will look at what NIST does regarding asset identification, focusing on CIP-002, not CIP-003.

This discussion provided guidance to Jackie and William to develop their approaches for review in February. Jackie noted she would be working with other members in developing the paper. William will look at how NIST can be tailored to fit with the CIP standards, while Jackie will look at how the CIP standards can be adopted into the NIST framework. Both will be brought together to see if and how a hybrid might work effectively. Both products will be circulated before the next face-to-face meeting in early February.

The SDT must sign off on the edits by the end of the next meeting in Phoenix to meet the proposed schedule for Phase I. The facilitators reviewed the schedule for the meetings through June 2009.

The meeting was adjourned at 11 a.m. on January 9, 2009.

Fifth Meeting Summary,
January 7–9, 2009
Phoenix, Arizona

I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair and Vice Chair welcomed the members and asked NERC staff David Taylor 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*).

David Taylor 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.

The Chair noted the December 4–5, 2008 meeting summary had been circulated to members in advance of the meeting. The team unanimously accepted the meeting summary.

II. TECHNICAL FEASIBILITY EXCEPTION- UPDATE, REVIEW AND REFINEMENT

Scott Mix provided an update on the Technical Feasibility Exception process since
The Technical Feasibility Exception (TFE) process is based on discussion with utility management. The process is not about the technical requirements and standards that the SDT is addressing, but it is more about whether compliance has been met; compliance is more than just the audit process. TFE was intended to address the issues where compliance could not be met quickly, thereby allowing for good reason to be technically out of compliance while significant issues can be addressed.

The TFE White Paper is being reviewed by NERC management. Compliance and Legal counsel were sought concerning how the white paper should be positioned and what it would mean to enforcement. It needs its own vetting process within NERC, and it may require modification to the Compliance Monitoring and Evaluation Program (CMEP). Changes to the CMEP are applicable across all of NERC's standards, so the TFE needs to well thought through and vetted within NERC.

Mike Assante, Chief Security Officer at NERC, has agreed to sponsor the TFE through the compliance process at NERC. Scott Mix will work with NERC Management to determine the best approach for getting this done.

Member Comments

- Is there a schedule for getting something to NERC's Mike Assante? Still missing legal information on how it can be done.
- This is an important issue linked to the removal of reasonable business judgment language in Phase I draft changes.

III. PHASE I INDUSTRY COMMENT and SDT RESPONSES

A. Overview of and Response to Phase I Comments on the SDT Standards

Kevin Perry provided a preliminary overview of the 119 pages of comments received from the 46 industry respondents. The comments were organized by NERC staff, and the latest set of comments was released to the SDT on January 7th. In summary, there were:

- No show stoppers
- Lots of duplication in the comments received
- Some comments cross multiple standards with common concerns such as:
  - Compliance Enforcement Authority
  - "a" vs. "the" senior manager and the delegation of authority
- New compliance language received lots of comments and maybe confusing to industry
- Confusion regarding data retention requirements warrants further discussion

Mr. Perry recommended that the Compliance team pay close attention to the new compliance wording so as to avoid the possibility of impact on all of the cyber security standards.

B. SDT Approach for Reviewing Phase I Comments

The SDT reviewed several approaches to responding to the Phase I comments on the cyber security standards. The preferred approach was to break up into small working groups to review an assigned grouping of standards in parallel. There was agreement to begin the Phase II discussion with the full SDT following the development and agreement on responses to Phase I comments. Following the small group breakouts, the full group would meet to discuss the findings and responses from each of the small working groups. Any cross-references or duplicative responses would be addressed and made consistent during this group review session.

The SDT agreed the Industry Comments need to be addressed in January 2009 through the face-to-face meeting and WebEx that were scheduled. The plan was to have the responses ready for review by NERC by the February 2–4, 2009 meeting for group adoption and eventual posting. Some of the SDT member overview comments included:

1. Many comments could be contentious and caution should be taken such that we answer comments at face value and not be drawn into the arguments.
2. Avoid getting drawn into discussing the Aurora incident; it is out of scope for the SDT.

3. A lot of the issues will be considered in Phase II; our response needs to indicate that the commenter should review their concern when Phase II documents are published for industry review and comment. An appropriate response may be "we will consider the comment in Phase II".
4. We will receive comments during the ballot period that we will need to respond to — hopefully the highly contentious issues are identified now before sending out the Phase I standards for ballot.
5. A "significant" change to a standard versus a "minor" change is a judgment call initially made by SDT and reviewed by the NERC Standards Manager (Maureen Long).
6. If we make a significant change to what's already been published, we'll have to seek comments again.
7. If we do not change the requirement but move it to a different standard, is that a significant change? Some clarification may be needed.
8. The plan is to issue the responses to the industry comments without requiring another round of industry comments.
9. If we receive a particularly contentious comment, consider removing the item for further consideration in Phase II.
10. Compliance comments and issues should be addressed by the Compliance small group which will have one SDT member participating.
11. Keep responses short and concise; don't water it down or get involved in long explanations; take the issue on in the appropriate language.
12. Point to reference documents, where appropriate, to address confusion about what some requirements mean.
13. Put the background material into the responses and refer to it, if needed.
14. A suggestion was made to include an introduction to the standards comments response document that describes the approach and what is being accomplished in Phase I and that the major issues will be addressed in Phase II.

C. Small Working Groups

Six small working groups were formed to review the industry comments and to develop the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP standards. The six groups and the SDT members participating included:

Working Group Assignments

CIP Standard No.	Questions Nos.	Assignments/Volunteers
002 & 003	Q1 & Q2	Jeri Brewer/Gerald Freese/Dave Norton/Dave Revill
004 & 007	Q3 & Q6	Chris Peters/Keith Stouffer/Mike

		Winters/William Winters
005 & 006	Q4 & Q5	John Varnell/ John Lim/ Rich Kinas/Scott Fixmer/Scott Rosenberger
008 & 009	Q7 & Q8	Tom Hofstetter/Joe Doetzel/Kevin Sherlin
Compliance	ALL Qs	Roger Lampila/Todd Thompson/Jackie Collett
Implementation	Q9, Q10, Q11, Q12	Kevin Perry/Scott Mix/Phil Huff
Q13	Q13	Tom Hofstetter and various small groups

The SDT agreed that whatever was not completed by the end of this meeting (January 7–9, 2009) could be taken up in the WebEx calls scheduled for January 15th and January 21st.

The members of each small working group were asked to consider the following in presenting their findings to the full group:

- Present substantive issues and responses from most to least contentious (10-15 total minutes for each small group report);
- The full SDT will focus on most contentious issues to confirm response(s); and
- Small groups may reconvene to refine responses.

The WebEx was re-initiated after lunch. The facilitator reviewed the expectations for the group reports with a focus on the most contentious or substantive issues that will need full group input for possible additional refinement. The small group reports were brief with an opportunity for groups to revise their work.

1. **Questions 1 and 2 (CIP 002 & 003)**
   Three sets of substantive issues were presented by the small group:

   1. Concern about assigning a senior manager in CIP-003 rather than in CIP-002.
   2. Clarify delegation of senior manger responsibilities
   3. Industry concern about the responsibility of a senior manager vs. a responsible entity (accountability issue?)

   SDT members noted there was some confusion over how to delegate responsibilities. For example, does the Senior Manager have the authority to: assign specific actions; identify which responsibilities will be delegated; document only those delegations assigned to each delegate; delegate authority for specific actions (added) “assigned to the senior manager” to a named delegate or delegates.

Other items the small group proposed for changes included:

- Delete "business phone" information. Yes
- Use "calendar days" throughout CIP-002 to 009.
- Add: "assigned to the senior manager" to a named delegate or delegates.

An SDT straw poll was taken to test support for adding/deleting this language to the requirement: *(Result: 7 for; 10 against, falling short of 75% support).* As a result of poll, the small group would draft responses consistent with this direction back to those offering the language in their comments.

2. **Questions 3 and 6 (CIP-004 and CIP-007)**
Substantive issues raised by the small group and discussed by the SDT included the following:

- How should the SDT respond to comments on addressing ambiguity in "specified circumstances"? SDT should answer that the language was included as directed in FERC Order 706.
- The SDT agreed they need to be specific in responses, not necessarily clarifying, but more explicit about what the drafting team will do with the issue raised.
- Don't change any language, but specify where the wording came from.
- Phase II will not change the language either.
- We should be careful about what we are promising to do in Phase II.
- Leave first sentence of the response as is and refine second sentence into a shorter version without promising future action
- SDT needs to avoid creating any linkages between guidance and standards.

The small group highlighted the following key items for discussion:

1. For R3 — need to specify critical assets. Added access "to critical cyber assets" - much the same reference in R2 — consistency issue
2. Added "all" in front of "other" cyber assets to remove any potential ambiguity. Need to be consistent across the different standards — use the same terminology

A SDT straw poll was taken to test adding securing "all" Cyber Assets within an ESP: (*10 yes; 8 no falling short of 75 percent support).* As a result of the poll, the guidance for the small group was to respond that these changes will be addressed in Phase II.

The SDT agreed not to take out "acceptance of risk" which did not make a substantive change but review of the response for group support. Recommendation is to consider language modification, residual risk analysis would demonstrate that an entity has

exercised due diligence when compensation measures have been applied. The SDT agreed that the response should be that the analysis will be considered in development of the technical feasibility (TFE) process.

Within the measures the team initially agreed with changing M2 to make it consistent with other measures, but suggest alternative language to add "and records" to M2 — (make available documentation "and records of its ports and services process" as specified in Requirement R2). SDT agreed to remove "and records" in order to limit the "heartburn". The SDT could revisit this in Phase 2?

A SDT straw poll taken to test if there support for adding the language. (*7 yes; 11 no falling short of 75 percent support)*. As a result of the poll, the guidance for the small group was to respond that these changes will be addressed in Phase II

The team may need to re-explain in the responses the need for the Phase I changes to meet the June audit deadline set by FERC Order when the response document is sent out for comment.

3. **Questions 4 and 5 (CIP-005 and CIP-006)**
Substantive Issues:

   a. Substitute "subsequent" phases for Phase II; "subsequent" phases anticipate significant changes

   b. Intent is to include only devices that perform access control or monitoring, not those devices that are receiving alerts

   c. Only a few real changes suggested and agreed to:

      - Change "maintain and implement" to "implement and maintain"
      - "Continuous" is a clarification of active escort and SDT agreed not to remove it from the requirement.
      - Agree that R1.4 should reference R4 and not R3
      - Competing authorities is outside the scope of the SDT – offer to refer it to appropriate entity (NERC)
      - Reliability standards only prescribe what and not how

   d. Is there a more positive way of asking commenters to resubmit during the next phase?

   e. In Phase II, the SDT will need to address differences between logging and monitoring/

   f. Use of "documents" versus "documentation" – need to be consistent in use

4. **Questions 7 and 8 (CIP-008 and CIP-009)**
    a. Concern with the addition of the word "dated" into the measures
    b. CIP 009-02 R3 missed the mark
    c. CIP 008-02 confusing wording

Actions:

a. "Dated": Remove the word "dated" from the measures.

b. CIP-009-02 R3:
- Rewrite to meet intent of FERC Order 706 (P731)
- Change control — updates shall be completed within 30 days and communicated within 90 calendar days (What is meant by "completed"?)
- Subsequent discussions led to the decision to wait to make any changes until Phase II development of the CIP Standards.

c. CIP-008-02 R1.3 to R1.6:
- Remove "process for" from each requirement
- R1.5 and R1.6 add annual testing of the response plan
- *Comments:*
    - Add to the compliance section as additional guidance?
    - Is this a major change requiring submittal for further comments?
    - Putting it in as additional compliance guidance - is it a major or minor modification to the standard?
    - This comment is not related to a change made in the last revision to the standards, but rather is a new additional item. These changes should be addressed as part of Phase II
    - Do we need to weigh the number of commenters making the comment that this section is confusing?
- Subsequent discussion to accept these comments or pull them for consideration in Phase II led to the conclusion to wait until Phase II. A good strawman will be needed to start the process at that time.

5. **Questions 9 to 12 (Implementation)**
    Actions to be taken:
    1. Update Implementation Tables
    2. Modify the SDT implementation plan to clarify emergency provision
    3. Change category 3
    4. Change #3 to add "cyber"
    5. Reference "other" CA rather than "non-critical" CA
    6. Modify timeframe to 18 months after the new CCA is identified
    7. Update Table 2 to reflect the addition of two new requirements

8. Any further updates to Table 2

Decisions:

a. Implementation plan as a separate document — consider incorporating in subsequent revisions

b. Guidelines for identifying CA and CCA are being developed

c. Six months is reasonable — the SDT agreed to leave it and not change it as requested to nine months

d. Nuclear facilities are out of the scope of this SDT group

Explanations:

- "In the event of a merger or acquisition of a company, … allow one year for the programs to be harmonized." If one party has a program then continue it while merging, if they have competing programs, then take a year to sort it out – this is a response to a comment, not making any changes to standard.
- Concern about how this applies when a holding company owns separately registered entities — will address by revising language here
- Reviewed items "tossed over the wall" to the Compliance small group

Proposed effective date in implementation plan — add "compliant" to clarify from "auditably compliant". There was no opposition. There was a test to leave without "compliant" which concluded with no objection. Why does title include "proposed"? Not adopted yet and consistent with other implementation plans

6. Compliance Issues (All CIPs)

- The wording in Compliance Section 1.1.1 does not specify who is responsible for the enforcement – not changing it at this time but probably will need to – have sent it to NERC (Maureen) for possible clarification
- Do the terms ERO and Compliance Enforcement Authority need to be defined in the glossary? They are already defined in the Rules of Procedure of NERC, which is hierarchically higher in terms of precedence of documentation, and therefore governs the definition - is not needed in the standards glossary
- Can we just add the same definition to the glossary? Keep response simple here that definition is already covered in the Rules of Procedure.
- "Dated" – do we revise the measures for all standards to include "dated"?
  - (Comment: - In phase I, leave it like it is – revisit in Phase II)
- Reinstate "duly authorized exceptions will not result in non-compliance"?
  - Referring back to NERC for follow up
- "In conjunction" leaves open possible interpretation – referred back to NERC

Jackie will review the rest of the compliance issues, but expects most new comments will be repeats from responses covered above. Jackie will flag any additional issues that the group may need to address.

7. **Question 13 (All CIPs)**
   Tom Hofstetter described how he assigned many of the comments to the appropriate small group. The small groups will need to tag or segregate their responses to Question 13 items so they can be pulled out to include as a set of responses under Question 13.

   Tom reviewed a few basic responses that he proposes to comments that are not related to other questions or small groups.

IV. NERC System Protection and Control Presentation (Jon Sykes)

Scott Mix introduced John Sykes, Vice Chair of the NERC System Protection and Control Subcommittee, which is looking at redundancy in control and protection systems, as an aspect of critical asset protection. They are early in their process of review.

The NERC SPCS has written a technical white paper, a proposed working paper for a standard, and has prepared the presentation. It took two an a half years to get to this point, and the SPCS need lots of industry input because of the high potential cost to the industry.

The major topic of discussion was on the methods for determining risk. Do we write a prescriptive standard or a performance-based standard? Key initial question, helped decide on the performance based approach.

Defined "redundancy", and reviewed protection system performance requirements Methodology to determine adequate redundancy of a Protection System:

- Determine redundancy of the PS
- Ascertain the performance of the PS
- Compare protection systems performance with electric system performance requirements in the TPL standards
- Mitigate all performance shortfalls

V. White Paper Discussions for Phase II

Stu Langton introduced a review of the Phase II White Paper process. He reviewed discussion from the previous SDT meeting in Washington where we came away with proposal to prepare and review two straw proposals, one starting from the CIP standards perspective and looking to incorporate applicable NIST concepts and the other starting from the NIST standards perspective and looking to incorporate CIP concepts.

Jackie Collett took a look at the NIST 800-53 standard and sees promise, but she also sees aspects of the standard that may cause concern for electric power systems. Jackie reviewed her take on the original intent of the NERC CIP 002 Standard.

William Winters offered initial thoughts on his approach from NIST, and how he might address some of the gaps in the standards but recognizing the concerns the industry may have with the NIST risk assessment approach, particularly cost. Bill will look at what NIST does regarding asset identification, focusing on CIP-002, not CIP-003. Some of the items addressed were:

- Concerns expressed by members about the disincentive for including critical assets, particularly for purposes of audits
- NIST may allow for gradations of identification, but that can complicate compliance – will the NIST approach work in the end?
- Energy Act 2005 and FERC announcements have come subsequent to the drafting of the standards which were written for data centers - industry concern about the cost and need for the identification of the critical assets
- Understand where and why we are where we are today to help figure out how to avoid potential industry refection – if industry does not accept, then FERC will do something because they now have clear Congressional support to do something
- Change in administration attitude about the need for industry regulation – we need to do a better job of educating the industry on the cyber risk in order to get their support for changes and limit the gaming – people want to do the right thing, if they understand why
- NERC SDT is focused on critical assets for the bulk power system, but the NIST framework covers the whole spectrum of systems used by the federal system.
- Generation aspect does not necessarily include transmission – we need to understand the different needs but be sure to include both – one size will not fit all for different systems
- Homeland Security list exists – need to resolve how industry list supports this other broader list
- ISA 99 takes a multi-level approach to security
- Identify the cyber assets that do x, y and z – then if it fails what bad happens – that identifies critical cyber assets system wide – is the information flow essential, follow out to find boundary, even where it crosses company boundaries – need to get away from applying physical engineering to the flow of information
- How do we reorganize what we consider critical?

This discussion provided guidance to Jackie and William to develop their approaches for review in February. Jackie noted she would be working with other members in developing the paper.

Should the approaches be combined now for review next time? Or parallel approaches to be merged later? Jackie envisioned parallel approaches to then be compared, and William agreed. Also they agreed that the items/issues identified are the starting points to be addressed. William will look at how NIST can be tailored to fit with the CIP standards, while Jackie will look at how the CIP Standards can be adopted into the NIST framework. Both will be brought together to see if and how a hybrid might work effectively.

Both products will be circulated before the next face-to-face meeting in early February. Some manner of blending will occur — just a matter of how much, however no one is saying start over from scratch. They will review and discuss the balance and trade-offs especially from an audit perspective. Five issue areas will be used by Jackie as part of the problem statement.

VI. Wrap-Up and Next Steps

The SDT must sign off on the edits by the end of the next meeting to meet the proposed schedule for Phase I. The next meeting is scheduled at the downtown Phoenix Hyatt Regency, please plan on staying the full meeting time, and especially try to stick around for the afternoon of the third day.

Beyond the February 2–4, 2009 meeting in Phoenix:

- February 18–19, 2009 in Fairfax, VA (ICFI Offices)
- March 10, 2009 Workshop
  - Progress at the next few meeting will help move us toward preparations for that workshop. Need to work in February to prepare for the workshop, which is preliminarily scheduled in conjunction with the March 10–12, 2009 SDT Meeting in the Orlando or Tampa area.
  - Purpose of the Workshop is to broaden our outreach and enlist review and input from cyber security experts in other industries as well as the electric industry.
  - The workshop will lead to a presentation to the NERC MRC on or about May 1, 2009.
- April 14–16, 2009 in Charlotte (Duke Energy)
- May 14–15, 2009 in Boulder City, NV (Bureau of Reclamation)
- June 17–18, 2009 in Manitoba (Manitoba Hydro)

Web meetings are scheduled approximately one week following each SDT meeting. Industry Webinar meetings are also planned to keep the industry informed on the progress of the Cyber Standards development.

The meeting was adjourned at 11 a.m. on January 9, 2009.

Appendix #1

Revised Meeting Agenda

Arizona Public Service Deer Valley Campus

Wednesday January 7, 2009

1:00 p.m. **Welcome and Opening Remarks — Jeri Domingo-Brewer and Kevin Perry**

a. Roll Call
b. NERC Antitrust Compliance Guidelines
c. FSU/FCRC Review of December meeting and adoption of December 4–5 Meeting Summary

1:15 **Review of Meeting Objectives and Agenda — Jeri Domingo and Bob Jones**

1:20 **Organizational Issues and Review of Phase 1 and early Phase II Schedule — Stuart Langton**

- Review of Phase 1 — Work-plan, January — May 2009 including small group proposal
- Review of Phase 2 — January–June, 2009 — including CIP-002 conceptual approach and industry input and feedback.

2:00 **Overview of Phase I Industry Responses — Number and Issues and Procedure Going Forward — Kevin Perry**

2:30 **Technical Feasibility Exception (TFE) — Briefing on NERC Review and Proposal Going Forward — Scott Mix**

3:00 **Break**

3:15 **TFE White Paper — Review of Changes and Additional Suggestions**

4:00 **Phase I Comment Review and Refinement — Full SDT Discussion of Cross Cutting Issues**

4:50 **Summary of Day One Outcomes and Review of Day Two Agenda**

5:00 **Recess**

Thursday January 8, 2009

8:00 **Welcome — Agenda Review and Review of Day One Results**

8:10 **Phase I Comment Review and Refinement- Plenary Discussion of Overall and Cross Cutting Issues**

9:00 **Break**

9:10 **Possible Small Group Breakouts — Review and Draft Responses**

12:00 **Working Lunch *(Return to plenary meeting at 12:45)***

12:45 **Initial Small Group Reports on Draft Responses and Full SDT Discussion**

2:45 **Break**

3:00	**Initial Small Group Reports on Draft Responses and Full SDT Discussion**
4:20	**Next Steps for Drafting Group WebEx Meetings in preparation for February 2–3, 2009 Meeting**
4:50	**Summary of Day Two Outcomes and Review of Day Three Agenda**
5:00	**Recess**

Friday January 9, 2009

8:00	**Welcome and Agenda Review**
8:10	**Learning from Other Initiatives — John Sykes, NERC System Protection and Control Task Force**
9:00	**SDT Discussion of Implications for Phase II 002 Critical Asset Identification**
10:00	**Break**
10:15	**Phase II White Paper Development — Early Thoughts and Preview and Questions of the SDT to aid in the drafting- Jackie Collette and William Winters**
11:30	**Assignments — Next Steps and Review of Work-plan**
12:00	**Adjourn**

Appendix # 2

Attendees List
January 7–9, 2009

Attending in Person — SDT Members

1 **Jeri Domingo-Brewer, Chair**	U.S. Bureau of Reclamation
2. Jackie Collett	Manitoba Hydro
3. Joe Doetzl	Manager, Information Security, Kansas City Power & Light Co. (Dec 4, in room, Dec 5 on phone)
4. Tom Hoffstetter	Midwest ISO, Inc
5. Scott Fixmer	Senior Security Analyst Exelon Corporate Security, Exelon Corp. (in room Dec 4, by phone Dec 5)
6. Gerald S. Freese	Director, Enterprise Information Security America Electric Power
7. Phillip Huff	Arkansas Electric Coop Corporation
8. Richard Kinas	Orlando Utilities Commission
9. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
10. David Norton	Policy Consultant, CIPEnergy Corporation
11. **Kevin B. Perry, Vice Chair**	Director, IT-Infrastructure, Southwest Power Pool
12. Christopher A. Peters	ICF International
13. David S. Revill	Georgia Transmission Corporation
14. Scott Rosenberger	Luminant Energy
15.Kevin Sherlin	Sacramento Municipal Utility District (Day 2)
16. Keith Stouffer	National Institute of Standards & Technology
17. John D. Varnell	Technology Director, Tenaska Power Services Co.
18.Michael Winters	Hydro One
19. William Winters	Arizona Public Service.
1. Roger Lampilla	NERC
2. David Taylor	NERC
3. Scott R. Mix	NERC
4. Todd Thompson	NERC
7. Robert Jones	FSU/FCRC Consensus Center Feb 3-4
8. Hal Beardall	FSU/FCRC Consensus Center Feb 2-4
9. Stuart Langton	FSU/FCRC Consensus Center
10. Joe Bucciero	Bucciero Consulting LLC

SDT Members Attending via WebEx and Phone

20. Jay S. Cribb	Southern Company Services, Inc.
21. Sharon Edwards	Project Manager, Duke Energy *Jan. 7.*
22.Jonathan Stanford	Bonneville Power Administration

SDT Members Not Attending

Bryan Singer	Kenexis Consulting Corp.

Appendix # 3

JANUARY — JUNE 2009 DRAFT SDT SCHEDULE

NOTE: Below are draft considerations developed by the facilitators in consultation with the Chair, Vice Chair and NERC staff and following the December SDT NERC Communication Plan briefing and Phase 1 Webinar on December 16. The facilitators also reviewed the SDT criteria for a "roadmap approach" to revising the CIP standards discussed and refined in Little Rock at its November, 2008 meeting (See pp 4 below for a list of the criteria) These considerations were used to construct a draft schedule for the SDT for the first half of 2009.

Short Term 2009 Schedule Draft Considerations

1. Follow the ANSI standard development process but use creative ways to efficiently secure input from the industry on emerging concepts and approaches to the CIP standards.
2. Seek creative ways to get advice and input to the SDT from experts in cyber security.
3. Seek creative ways to get focused input from industry stakeholders.
4. Take advantage of input opportunities from related NERC committees that will be meeting in the first half of 2009 (e.g. working with the NERC Members Representative Committee, CIPC, BOT, and industry committees such as the Electricity Sector Coordinating Council, etc.)
5. Seek, as soon as possible but no later than late Spring, 2009, to establish a consensus on the way forward for the SDT in its efforts to revise the CIP standards.
6. Track any follow up to the "Securing Cyberspace for the 44th Presidency" report of the Commission on Cyber security for the 44th President.

SDT Draft Schedule — January–June 2009

Overview

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommittees WebEx Meetings
- 1 Cyber Expert Workshop (March 10 or 11, 2009)
- 1 NERC CIPC presentation? (Feb. 9, 2009)
- Industry Comments on CIP 002 White Paper (April 17–June 3)
- 1 NERC Members Representative Committee, May 1, 2009
- Other Meetings?

SDT Draft Schedule — January–June, 2009

1. January 7–9 SDT Meeting — Phoenix, AZ ½–1/½ day format — Wednesday–Friday

- Review of Technical Feasibility Exceptions white paper
- Review of Industry Comments on Phase 1 products- Establish and convene small groups
- Initial Review of Phase 2 White papers

January 15 — WebEx meeting(s)

- Small group draft responses to industry.

January 21 — WebEx meeting(s)

- Small group draft responses to industry.

2. February 2–4, 2009 SDT Meeting — Phoenix, AZ, ½–1/½ day format — Monday–Wednesday

- Review of Small Group responses and recommendations on Industry comments and adopt draft of Phase 1 products, as revised, for review by NERC/Maureen.
- Review of Phase 2 White papers and Testing of a Phase 2 CIP 002 concept going forward

February 9, 2009 — CIPC Meeting — Update on SDT Progress and Input?

February 11 — WebEx meeting?

- Phase 2 drafting concept group?

3. February 18–19, 2009 SDT Meeting — Boulder City, NV

- Review of Maureen's comments and adoption of Phase 1 products for balloting.
- Further discussion and adoption of a draft Phase 2 CIP 002 Concept for review by experts and stakeholders in March and beyond.

February 25 — WebEx meeting(s)

- Phase 2 drafting concept group?
- Development of Phase 2 CIP 002 Workshop for review by experts and stakeholders

4. March 10–11, 2009 SDT Meeting — Tampa, FL, 2-day format

- Invited Cyber Security Experts join SDT in a workshop to provide expert feedback to draft CIP 002 concept.
- Further SDT refinement of the CIP 002 proposed concept

March NERC Balloting on Phase 1 Products

March 18 — WebEx meeting(s)

- Phase 2 drafting concept group?

5. April 14–16, SDT Meeting, Charlotte NC — ½–1/½ day format. Wednesday-Friday

- Continue review and refinement of 002 concept and adopt White Paper on CIP 002 concept for Industry Comment

Industry Comment Period on White Paper — 45-days (April 17–June 3)

*May 1, **NERC Member Representative Committee**, Presentation of the Phase 2 CIP 002 Approach for MRC input. (Agenda item, Possible Workshop?)*

6. May 13–14 — SDT Meeting — Dallas, TX, 2-day format

- Review and respond to MRC input and further SDT refinement of the CIP 002 proposed concept and SDT CIP roadmap.
- Organize SDT in subcommittees to begin effort to draft revisions to CIP 003-008 or to address key issue areas.

June — following June 3 — WebEx meeting(s)

- SDT subcommittee meetings to review and draft responses to Industry comments on the CIP 002 concept.

7. June 17–18, SDT Meeting — Location TBD —2-day format

- Review Subcommittee responses to Industry comments on 002 approach
- Charge subcommittees and conduct organizational meetings
- Subcommittees meet to draft revisions to CIP 003-008

June — WebEx meeting

- SDT Subcommittee meetings

July–December, 2009 — SDT and subcommittees meet and continue CIP drafting

2nd DRAFT PHASE 2 ROADMAP APPROACH ASSESSMENT CRITERIA

(Presented, Revised, and Added to by SDT in its review on November 14, 2008)

1. The approach is consistent with the SDT purpose statement and is responsive to the FERC 706 directives and the SAR.
2. The approach is achievable given the SDT schedule and work plan.
3. The approach does most to advance and enhance cyber security in the BES.
4. The approach helps the SDT address the foundational issues with the current standards.
5. The approach is capable of implementation.
6. The approach is capable of improving compliance.
7. The approach helps protect the current investments and wherever possible builds on what has already been done.
8. The approach helps to identify and mitigate risk on an ongoing basis.
9. The approach balances a “systems” orientation with a “facilities” orientation to asset protection.
10. The approach is capable of being extended into related interests by others (distribution, AMI, Smart Grid, etc.).
11. The approach enables the industry to provide the appropriate level of security (i.e. not over securing nor under securing the BES cyber assets).

12. The approach allows for discrimination among and targeting the various types of infrastructure that support the BES

Appendix # 4

NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

Appendix # 5

Below is a link to all of the documents reviewed by the SDT during the full team discussions in Washington D.C. as well as Phase 1 SDT Products:

Adopted Unanimously, November 13, 2008

Cyber Security for Order 706 Standard Drafting Team

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 percent acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75 percent 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 percent 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 percent 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 or 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 percent of the appointed members being present (simple majority). The ream 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 percent 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/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

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.

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.

Regarding Risk Management

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 Docket No. RM06-22-000 - 71 -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.

254. Commenters raise a number of topics that they believe should be addressed in the NERC guidance, such as how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by an adversary. We believe these are all appropriate topics to be addressed and direct the ERO to consider these commenter concerns when developing the guidance.

255. The Commission proposed in the CIP NOPR that the ERO and Regional Entities provide reasonable technical support to relatively smaller entities that may have difficulty determining whether a particular asset is critical because, for example, the impact of the facility may be dependent on their connection with a transmission owner or operator. While we believe that there is a need to assist entities that lack a wide-area view, we are mindful of the ERO's concern that it would place an undue burden on it and the Regional Entities. If the ERO believes that it and the Regional Entities do not have sufficient resources to take on this responsibility, it should designate another type of entity with a wide-area view, such as a reliability coordinator, to provide needed assistance. This approach is consistent with our determination (discussed later in this Final Rule) regarding the external review of critical asset lists. Accordingly, we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.

256. Regarding MidAmerican's comments on use of the N minus 1 criterion when applying a risk-based assessment methodology to the identification of critical assets, we agree with MidAmerican that an N minus 1 criterion is not an appropriate risk-based assessment methodology for identifying critical assets. While the N minus 1 criterion may be appropriate in transmission planning, use of an N minus 1 criterion for the risk based assessment in CIP-002-1 would result in the nonsensical result that no substations or generating plants need to be protected from cyber events. A cyber attack can strike multiple assets simultaneously, and a cyber attack can cause damage to an asset for such a time period that other asset outages may occur before the damaged asset can be returned to service. Thus, the fact that the system was developed to withstand the loss of any single asset should not be the basis for not protecting that asset. Also, we note that the definition of "critical assets" is focused on the criticality of the asset, not the Docket No. RM06-22-000 - 72 - likelihood of an outage. Based on this reasoning, in response to US Power, we clarify that a generator should not assume that none of its individual generating assets would be regarded "critical" to the Bulk-Power System.**84**

257. With regard to Xcel's request for clarification regarding the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4, we direct the ERO to consider this clarification in its Reliability Standards development process.

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal "feedback loop" to assist the industry in developing policies and procedures.**85**

FN84 Further, Requirement R.1.2.3 provides that the risk-based assessment must consider "generation resources that support the reliable operation" of the Bulk-Power System. This language indicates that certain generation facilities, and presumably some facilities within a region identified as critical, must be considered in an assessment. Beyond this, we leave it to the ERO to provide sufficient guidelines to inform generation owners and operators on how to determine whether it should identify a facility as a critical asset. As discussed later in the Final Rule, the Commission will monitor and evaluate the outcome of this endeavor – the list of critical assets.

FN85 Consistent with our approach in Order No. 693, the ERO should address NOPR comments suggesting specific new improvements to the CIP Reliability Standards. The Commission, however, does not direct any outcome other than that the comments receive consideration. See Order No. 693 at P 188.

272. Based on the range of comments received on this topic, the Commission is convinced that the consideration and designation of various types of data as a critical asset or critical cyber asset pursuant to CIP-002-1 is an area that could benefit from Docket No. RM06-22-000 - 76 -greater clarity and guidance from the ERO. Accordingly, the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset. In doing so, the ERO should consider Juniper's comments. Further, the Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.
273. The Commission also agrees with ISO-NE that experience in the implementation of the CIP Reliability Standards may indicate a need to further address this topic in a future proceeding.

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

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.