NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Revised Meeting Agenda

Cyber Security Order 706 SDT — Project 2008-06

January 7, 2009 | 1–5 p.m. PST
January 8, 2009 | 8 a.m.–5 p.m. PST
January 9, 2009 | 8 a.m.–noon PST
Arizona Public Service Deer Valley Campus
Black Canyon 3 Building (BC-3)
2133 W. Peoria Ave.
Phoenix, AZ (609-250-1117)

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**

noon **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**
noon	**Adjourn**

Cyber Security Order 706 SDT — Project 2008-06
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 Cybersecurity for the 44th President.

SDT Draft Schedule — January–June 2009

Overview

- 7 SDT Face-to-Face Meetings
- Multiple SDT subgroup and subcommitees 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 workplan.
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