NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

26th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Adopted Unanimously by the SDT on October 14, 2010

Winnipeg Manitoba

September 8, 2010, Wednesday - 8 AM to 6 PM CDT
September 9, 2010, Thursday - 8 AM to 6 PM CDT
September 10, 2010, Friday - 8 AM to 10 AM CDT

Robert Jones, Stuart Langton, and Hal Beardall
Facilitation and Meeting Design
FCRC Consensus Center, Florida State University

Joe Bucciero, Bucciero Consulting, LLC

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT September 8-10, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
26TH MEETING
September 8-10, 2010
Winnipeg, Manitoba

EXECUTIVE SUMMARY

On Wednesday morning, John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Winnipeg and thanked Jackie Collett and Manitoba Hydro for hosting the meeting. Jackie reviewed the logistics for the meeting. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call. Mr. Bucciero also reviewed the need to comply with NERC's Antitrust Guidelines each day of the meeting, and reminded all participants that the meeting has been publicly noticed and is open to the public. The meeting began with a quorum of 15 members in the room and 3 members participating by ReadyTalk conference call. John Lim reviewed the proposed meeting objectives; facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

On Thursday morning, the SDT unanimously adopted the August 10-13, 2010 Chicago SDT meeting summary and the August 26, 2010 SDT Conference Call Summary.

Vice Chair Phil Huff reviewed the note that the SDT leadership sent to Standards Committee Chair, Allen Mosher, regarding the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting in August 2010. The note calls for a NERC-led communications and industry outreach effort along with a posting of the CIP-010/CIP-011 standards in July 2011 and adoption of the standards by the NERC Board of Trustees in December 2011.

He also reviewed the CIP 002-4 schedule noting a Webinar has been scheduled for September 29, a week after the scheduled CIP 002-4 posting for a 45 day formal comment period. The SDT reviewed the Webinar preparation on Friday morning. In October the SDT will meet in Toronto and will be taking an initial look at the work of the Framework Sub-Team led by David Norton. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

The SDT heard industry updates and discussed the following: the process for the urgent action CIP 005; the CAN 7 revision and review; the formation of a national electric sector cyber security organization called NESCSO at NETL; the final release of the NIST IR7628 (termed as a "guideline" but treated in the Federal sector like a standard); the DHS Cyber Security Roadmap for critical infrastructure activities; and the October NERC annual standards meeting in St. Louis.

John Lim provided an overview of the work done by the CIP-002-4 drafting sub-team in refining the draft CIP 002-4 standard text following the Chicago meeting. The SDT reviewed and analyzed industry responses to the NERC Data Request as input to Attachment 1 of the CIP-002-4 standard, and reviewed and refined several associated documents including: an implementation plan, a guidance/reference document including rationales for Attachment 1 and a summary of industry informal comments on CIP-010 Attachment 2, on which CIP-002-4 Attachment 1 is based. Howard Gugel reviewed the process for posting CIP-002-4.

The SDT discussed the schedule for urgent action CIP-005, and it was clarified that it will be balloted separately, but will run in parallel with CIP-002-4. The revision to CIP-005-3 was posted for a 30-day pre-ballot review on August 18, 2010, and the draft CIP-005-4 standard is scheduled for a 10-day ballot period beginning on September 17, 2010. No recirculation ballot is planned.

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the initial analysis of industry responses to the draft NERC Data Request. Following some further clarification and discussion with several Data Request respondents, Howard reviewed with the SDT on Thursday the adjusted results in the number of assets in the low impact category (from around 1300 to around 530).

The SDT reviewed each section of the CIP 002-4 draft, and as needed, conducted straw polls on the acceptability of the language.

CIP 002-4 SDT Straw Polling and Decisions on Motions	***Yes***	***No***	***Abstain***	***%***
Requirements				
R2 as proposed by the Drafting Team	**20**	**0**		**100%**
Attachment 1 Criteria				
1.1 as proposed by the Drafting Team	10	5	4	
1.1 Alternative ("…aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."	13	6	2	
1.1 Choice #1 ("Use a numerical MW value that approximates the reserve sharing for each NERC region.")	7	9		44%
1.1 Choice #2 ("Use numerical MW value that approximates an average of the reserve sharing amounts across all regions")	12	6		67%
1.1 Choice #3 (Use the Reserve Sharing concept, rather than a MW value, but include additional descriptions supplied by Control Center experts	13	4		76%
1.1 Choice #4 ("Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting.")	10	5	4	
1.1 "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.	**19**	**0**		**100%**
1.2 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."	**13**	**2**	**4**	
1.5 As proposed by the Drafting Team	**11**	**3**	**5**	
1.5 Alternative *(Rich Kinas language)*	**1**	**17**	**0**	

1.5 *As rewritten*-The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.	**16**	**1**	**3**	
1.7 As proposed by the Drafting Team	**17**	**0**	**2**	
1.8 As proposed by the Drafting Team	**17**	**0**	**3**	
1.8 Alternative language (proposed by Jason Marshall)	0	18		
1.9 As proposed by the Drafting Team	19	0		
1.10 As proposed by the Drafting Team	18	0	3	
1.11 As proposed by the Drafting Team	20	0		
1.12 As proposed by the Drafting Team	20	0		
1.13 As proposed by the Drafting Team	18	2		
1.14 As proposed by the Drafting Team	16	2	2	
1.15 As proposed by the Drafting Team	15	2	2	
1.15 Delete "in an single interconnection"	6	12	1	
1.16 "Any facility declared by a regulatory agency to be critical to national security."	0	19	0	
1.17 "Any additional assets that the Responsible Entity deems appropriate to use."	17	3	0	
Motion to Approve Attachment 1 as Revised *(S. Edwards; 2nd D. Johnson)*	**18**	**1**		**95%**
Implementation Plan Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)	**18**	**0**	**0**	
Motion to Approve to Implementation Plan as Revised	**18**	**0**		
Motion to Approve CIP 002-4 Reference Document	**18**	**0**	**1**	
VSLs/VRFs as revised	**19**	**0**		
Cover Letter and Comment Form as revised	**19**	**0**		

The SDT reviewed a draft agenda and proposed assignments for an industry webinar on September 29 from 11:00 a.m. -1 p.m. on the CIP 002-4 filing, which the Chair outlined. Allen Mosher, Chair of the NERC Standards Committee will provide some introductory remarks in terms of the context and recent history of the SDT's efforts. It was noted that the presentations would be at a relatively high level with the intention of leaving sufficient time of the Webinar devoted to Q & A. There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard.

Dave Norton, Sub-Team lead, reported on the two meetings the Framework Sub-Team has convened. He suggested the context is that some in the industry stakeholders did not like what they saw with CIP-011, and the regulator doesn't think we have approached things consistently with the NIST 800-53 framework, thereby establishing a baseline at the outset. The Sub-Team has agreed that the SDT needs to answer the question, "what are we protecting and from who?" There are threats, vulnerabilities and impacts to consider but threats are hard to be clear on, and impacts have a lot of permutations. The Sub-Team is initially focusing on known vulnerabilities in the open information sources and posing the question: how can we use known vulnerabilities to link to specific standards (e.g., NIST IR volume 3, Chapter 7 treatment of vulnerabilities). The original CIP standard team learned that it is very difficult to write CIP requirements that address the old and new at the same time,

resulting in overkill for the old and leaving modern vulnerabilities unaddressed. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework for the CIP standards, and not a format. Ultimately this should lead to a format.

Dave Revill noted that when the SDT developed CIP-011, we identified requirements at the high impact level and forced the scoping elements on them. The Framework Sub-Team's idea is to start from the bottom and work up.

The Chair noted that the Framework Sub-Team will have a significant amount of agenda time during the Toronto SDT Meeting in October to bring the SDT up to date and engage them in discussion of the key issues. These discussions should provide guidance as the Sub-Team continues its efforts to bring back a framework that the SDT can review, refine, and adopt at its December 2010 meeting that will guide its work in 2011.

On Friday morning, the SDT reviewed the progress being made by the CIP-010 and CIP-011 sub-teams in summarizing industry responses and the Dallas workshop comments. The Chair thanked those sub-groups who had completed their tasks and asked all the sub-groups to complete their summaries by the SDT October meeting

The Chair reviewed the schedule for a SDT conference call meeting on Wednesday, September 15 from 10:00 a.m.-12:00 p.m. (eastern time) to review the final documents for posting that were not adopted at this meeting and to determine whether the SDT members, following review with their corporate senior management, wanted to revisit the SDT's previous decisions on whether to specifically include all nuclear generation as a criterion for assessment in CIP-002-4 Attachment 1.

The Toronto agenda was discussed and SDT member and host Rob Antonishen described the Toronto, Ontario venue for the meeting.

Meeting adjourned at 9:45 a.m. Friday, September 10, 2010

_____

Cyber Security Order 706 SDT- Project 2008-06
26TH MEETING SUMMARY
September 8-10, 2010
Winnipeg, Manitoba

I. AGENDA REVIEW, WORKPLAN SCHEDULE AND UPDATES

A. Agenda Review and Adoption of Meeting SDT Summaries

John Lim, Chair & Phil Huff, Vice Chair of the CSO 706 SDT welcomed members and other participants to Winnipeg and thanked Jackie Collett and Manitoba Hydro for hosting the meeting. Jackie covered logistics and noted a tour of the new energy efficient Manitoba Hydro building at the end of the day. Joe Bucciero conducted a roll call *(See Appendix #2)* and reviewed the antitrust and public meeting guidelines *(See Appendix #3)* with the meeting participants at the outset on each day. On Thursday morning, the SDT unanimously adopted the August 10-13, 2010 Chicago meeting summary and the August 26 SDT Conference Call Summary. The meeting began with a quorum of 15 members in the room and 3 members participating by Readytalk conference call. John Lim reviewed the proposed meeting objectives, the facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda.

B. Update on the CIP 002-4 and the 010 and 011 Development Schedule

Vice Chair Phil Huff reviewed the note that the SDT leadership sent to Standards Committee Chair, Allen Mosher, regarding the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting in August 2010. The note calls for a NERC-led communications and industry outreach effort along with a posting of the CIP-010/CIP-011 standards in July 2011 and adoption of the standards by the NERC Board of Trustees in December 2011.

He also reviewed the CIP 002-4 schedule noting a Webinar has been scheduled for September 29, a week after the scheduled CIP 002-4 posting for a 45 day formal comment period. The SDT reviewed the Webinar preparation on Friday morning. In October the SDT will meet in Toronto and will be taking an initial look at the work of the Framework Sub-Team led by David Norton. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

C. Updates on other related cyber security initiatives- *NERC Staff and SDT Members*

The SDT discussed the schedule for urgent action CIP-005, and it was clarified that it will be balloted separately, but will run in parallel with CIP-002-4. The revision to CIP-005-3 was posted for a 30-day

pre-ballot review on August 18, 2010, and the draft CIP-005-4 standard is scheduled for a 10-day ballot period beginning on September 17, 2010. No recirculation ballot is planned.

Scott Mix also noted that the CAN 7 was under review and was being prepared for review by NERC legal staff next week. Jim Brenton noted that CAN 5 is on track for implementation in October and that there are likely to be a lot of concern in the industry about this CAN.

The SDT heard industry updates and discussed the following: the process for the urgent action CIP 005; the CAN 7 revision and review; the formation of a national electric sector cyber security organization called NESCSO at NETL; the final release of the NIST IR7628 (termed as a "guideline" but treated in the Federal sector like a standard); the DHS Cyber Security Roadmap for critical infrastructure activities; and the October NERC annual standards meeting in St. Louis.

Keith Stouffer reported that last Thursday the NIST IR 7628 was finalized and is now available on the website for down load. He noted that while it is termed as a "guideline" it is treated in the Federal sector like a standard.

Gerry Freese noted the DHS Cyber Security Roadmap which provides guidance for critical infrastructure activities has been released for comment and indicated some concerns with load issues, interdependencies and other issues. It was noted that it was on the agenda for discussion at next week's CIPSE meeting. Sharon Edwards had read it and suggested there is some overlap with the work of the SDT. Scott Mix noted that Section 215 addresses the areas for which NERC can write enforceable standards.

Howard Gugel noted that at the October NERC annual standards meeting in St. Louis, he will make a presentation on the evolving work of the SDT on CIP-010 and CIP-011.

II. SDT CIP 002-4 DOCUMENT REVIEW

A. Overview and Process

John Lim provided an overview of the work done by the CIP-002-4 drafting sub-team in refining the draft CIP 002-4 standard text following the Chicago meeting. The SDT reviewed and analyzed industry responses to the NERC Data Request as input to Attachment 1 of the CIP-002-4 standard, and reviewed and refined several associated documents including: an implementation plan, a guidance/reference document including rationales for Attachment 1 and a summary of industry informal comments on CIP-010 Attachment 2, on which CIP-002-4 Attachment 1 is based. Howard Gugel reviewed the process for posting CIP-002-4.

Howard Gugel reviewed the process for posting CIP-002-4:

- The documents will be posted for 45-day formal comment period during which the first 30 days a ballot pool will be formed. On the 35th day, there will be a concurrent ballot for 10 days.
- Any comments received will require responses. With the short turnaround, NERC staff will assist the SDT in drafting strawman response document.
- The SDT will review the responses and determine whether to change any provision CIP-002-4 in Baltimore in November. NERC standards and legal staff will review and the response document will be posted.
- The 2nd ballot period will run for 10 days.
- The Team will respond to comments and post for a 3rd ballot in December

The SDT discussed the schedule and clarified whether urgent action CIP 005 will be a part of the CIP 002-4 etc posting. There will be a separate ballot on urgent action CIP 005-4 which will run parallel with CIP-002-4 and the ballot will open on September 20 for 10 days with no recirculation. If CIP-005 is turned down, then NERC would publish CIP 005-3 with conforming changes from CIP-002-4.

B. Briefing on the NERC Data Request Results

On Wednesday morning, NERC staff (Howard Gugel) reviewed with the SDT the initial analysis of industry responses to the draft NERC Data Request. *(See Appendix #4)* Following some further clarification and discussion with several Data Request respondents, Howard reviewed with the SDT on Thursday the adjusted results in the number of assets in the low impact category (from around 1300 to around 530). He also pointed out the new provision added to the Attachment #1 (the new 1.16) would be supported by the number of assets included in this category in the survey.

C. Review and Refinement of the CIP 002-4

The SDT reviewed each section of the CIP 002-4 draft, and as needed, conducted straw polls on the acceptability of the language. The final adopted text is included in Appendix #5. Below is a list of the straw polls and decisions reached by the SDT on the CIP 002-4 documents:

CIP 002-4 SDT Straw Polling and Decisions on Motions	*Yes*	*No*	*Abstain*	*%*
Requirements				
R2 as proposed by the Drafting Team	**20**	**0**		**100%**
Attachment 1 Criteria				
1.1 as proposed by the Drafting Team	10	5	4	
1.2 Alternative ("…aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."	13	6	2	
1.2 Choice #1 ("Use a numerical MW value that approximates the reserve sha each NERC region.")	7	9		44%
1.2 Choice #2 ("Use numerical MW value that approximates an average of the sharing amounts across all regions")	12	6		67%
1.2 Choice #3 (Use the Reserve Sharing concept, rather than a MW value, but additional descriptions supplied by Control Center experts	13	4		76%
1.2 Choice #4 ("Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting.")	10	5	4	
1.3 "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.	**19**	**0**		**100%**
1.3 Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."	**13**	**2**	**4**	
1.5 As proposed by the Drafting Team	**11**	**3**	**5**	
1.5 Alternative *(Rich Kinas language)*	**1**	**17**	**0**	
1.5 *As rewritten*-The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.	**16**	**1**	**3**	
1.7 As proposed by the Drafting Team	**17**	**0**	**2**	
1.8 As proposed by the Drafting Team	**17**	**0**	**3**	
1.8 Alternative language (proposed by Jason Marshall)	0	18		
1.9 As proposed by the Drafting Team	19	0		
1.10 As proposed by the Drafting Team	18	0	3	
1.11 As proposed by the Drafting Team	20	0		
1.12 As proposed by the Drafting Team	20	0		
1.13 As proposed by the Drafting Team	18	2		
1.14 As proposed by the Drafting Team	16	2	2	
1.15 As proposed by the Drafting Team	15	2	2	
1.15 Delete "in an single interconnection"	6	12	1	
1.16 **"**Any facility declared by a regulatory agency to be critical to national securi	0	19	0	
1.17 "Any additional assets that the Responsible Entity deems appropriate to use."	17	3	0	
Motion to Approve Attachment 1 as Revised *(S. Edwards; 2nd D. Johnson)*	**18**	**1**		**95%**
Implementation Plan Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)	**18**	**0**	**0**	
Motion to Approve to Implementation Plan as Revised	**18**	**0**		
Motion to Approve CIP 002-4 Reference Document	**18**	**0**	**1**	
VSLs/VRFs as revised	**19**	**0**		
Cover Letter and Comment Form as revised	**19**	**0**		

1. CIP 002-4 Requirements

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

SDT Comments

- R1 and R2- "updated as necessary"? What is the metric? "Where appropriate"? "Based on the annual review." A: "one calendar quarter after discovery of a new asset."
- "Annual" has been a thorn for the SDT for a long time.
- We should keep it the way it is using the "minimalist" rule for CIP 002-4.
- This also appears and would need to be changed in CIP 003-009.
- It is frustrating when we can make a simple change and improve the standards but don't.
- Have language in CIP 10 as well. Identified and addressed.
- Note that the SDT voted last time 17-0 to accept this language.
- The SDT should be careful of scope creep: on 002-4. Will fix and do correctly.

Howard Gugel 9/28/10 4:36 PM
Comment: Actually, we addressed the low hanging fruit initially.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets. The Responsible Entity shall review this list at least annually, and update it as necessary. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R2.2The Cyber Asset uses a routable protocol within a control center; or,

R 2.3The Cyber Asset is dial-up accessible.

SDT Comments on R2

- The drafting team added back" performing a function essential to the operation of the Critical Asset."
- R2 "Each" Place qualification ("within 15 minutes) at R2.4
- 15-minute criteria only applies to generation units.

- One of the following characteristics- place in a footnote? 'the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1 criterion 1.1 within 15 minutes.
- Intent of sub requirements- applied to the asset's identify at the generator. If below or equal they won't apply.
- A change will require changing all the numbering.
- All comfortable with proceeding with it as proposed?

SDT Straw Poll on R2 As Written

Yes	***No***	***Abstain***
20	**0**	**0**

2. Attachment 1 Criteria

Criterion 1.1

John Lim reviewed the minor changes made in 1.1 since Chicago. The SDT discussed and were polled for their support for 1.1 as written.

> **1.1. A generating unit or group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the CIP-002 is reviewed.**

SDT Straw Poll on 1.1 As Written

Yes	***No***	***Abstain***
10	**5**	**4**

The SDT's initial discussion of the proposed language in 1.1 noted concerns about: utilizing the concept of reserve sharing as a threshold value; the unintended consequence of placing pressure on entities to no carry additional reserve; referencing a term that will fluctuate over time; the difficulty to finding the number as demonstrated in the NERC date request responses; and introducing a new operational term ("planned Contingency Reserve") that does not appear in other standards.

Several potential options were identified including: gigawatt hours per year produced; tie to name plate ratings but address capacity using the test results required to run to demonstrate capacity referencing proposed Mod 24 standard); use contingency reserve to come up with a defensible number, but don't tie the 1.1 to a contingency reserve.

Following the ranking, the SDT discussed that if the contingency reserve is the value we are comparing then it needs clarification in terms of what it is and how it is determined and how to define a "group of generating units."

The SDT then reviewed concerns and support for the following alternative 1.1 language including: this is using the concept to derived a value; this figure is based on disturbance not reliability; having a bright line across each region may not make sense; this is an indirect way to identify critical assets; and bright lines should be readily available and clear for each entity. The SDT then polled support for the following:

> **Alternative 1.1: "Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 2000 MW."**

SDT Straw Poll on 1.1 As Re-written

Yes	***No***	***Abstain***
13	**6**	**2**

Sharon Edwards agreed to draft options for the SDT consideration on Thursday based on the discussion on Wednesday. She summarized the following four options for the SDT's consideration and recommended consideration of Options 1 and 3 to begin with. It was suggested that the SDT needs to make a decision on this and seek industry input through the comment and balloting process.

Choice #1 – Use a numerical MW value that approximates the reserve sharing for each NERC region: Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding the amount designated in the following table:

FRCC	900 MW	MW Value approximates the Reserve Sharing amount for that region *(Kinas)*
MRO	2200 MW	MW Value approximates the Reserve Sharing amount for that region (Collect)
NPCC	1200 MW	MW Value approximates the Reserve Sharing amount for that region *(Lim)*
RFC	2000 MW	MW Value approximates the Reserve Sharing amount for that region *(Marshall)*
SERC	1200 MW	MW Value approximates the Reserve Sharing amount for that region *(Revill)*
SPP	TBD *(KP)*	MW Value approximates the Reserve Sharing amount for that region *(Perry)*
ERCOT	2300 MW	MW Value approximates the Reserve Sharing amount for that region *(Brenton)*
WECC	TBD*(JVB)*	MW Value approximates the Reserve Sharing amount for that region

Sharon noted that this option allows regional flexibility in setting specific MW value but it is difficult to calculate for each region. The table figures were presented as initial approximations for region based on available information.

SDT Straw Poll on Choice #1

Yes	***No***	
7	**9**	**= 44%**

Comments on Choice #1before Poll

- The numbers are set by Reserve Sharing Group not by regions.
- The NPCC # doesn't reflect number for other areas within the NPCC.
- Need a number that does not change over time. Choice # 3 is more preferable if we can get away from new terms not seen yet by the industry.
- Concerns raised by members may make this problematic. Is 900 MW always critical?
- The table is intended to offer average approximations that can serve as the basis for bright lines. They do not represent an average of every BA in the region.
- 2300 may not be the ERCOT number.
- In favor of the table yesterday. Would still vote for that approach.

Choice #2 – Use numerical MW value that approximates an average of the reserve sharing amounts across all regions: Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

SDT Comments on Choice #2 before poll

- This is similar to approach with 2000MW. 1500-1600 MW table in Choice 1. Question of the values served by this. Over 900 doesn't work in Florida.
- 1500 MW will capture about 1/3 of generation in US.
- We have used 2000 so far here and elsewhere?
- To address the concern regarding FRCC, it can adopt a more stringent value based on their regional need.

SDT Straw Poll- Choice #2

Yes	***No***	
12	**6=**	**67%**

Comments after poll

- What is the basis of the table. It is a way of drawing a line in the sand.
- Here's how we drew the line.
- Get number out to industry to get reaction.

Choice #3 – Use the Reserve Sharing concept, rather than a MW value, but include additional descriptions supplied by Control Center experts. (*Note: No new definitions are being proposed.)* Each ~~generating unit or~~ group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months within the Reserve Sharing Group, or a Balancing Authority if it is

not a member of a Reserve Sharing Group, exceeding the lowest planned contingency reserve (Spinning plus Operating Reserves plus additional reserves) over the preceding 12 months at the time the Responsible Entity reviews its list of Critical Assets.

SDT Comments on Choice #3 before the poll

- Based on the SDT discussion yesterday, a little clarification/information (spinning plus) was added to the reserve sharing concept.
- There is a problem with ("spinning plus operating reserves). Concerned with defining this term.

SDT Straw Poll on Choice #3

Yes	***No***	
13	**4=**	**76%**

Comments on Choice #3 after poll

- Why can't we use the nameplate rating here? A: Nameplate is not always the operating capacity.
- How much precision do we need?
- Nameplate is like horsepower of a car.

Choice #4 – Use the Reserve Sharing concept, rather than a number, as it was proposed at the start of this meeting: Each ~~generating unit or~~ group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability in the preceding 12 months exceeding the lowest Contingency Reserve identified over the preceding 12 months by the Reserve Sharing Group or the Balancing Authority if it is not a member of a Reserve Sharing Group, at the time the Responsible Entity reviews its list of Critical Assets.

SDT Comments on Choice #4 before the poll

- This is the proposal reviewed and polled at start of meeting yesterday with the following results:

Yes	***No***	***Abstain***
10	**5**	**4**

The facilitators noted that both Choice #2 and Choice #3 garnered more than 2/3's support from the SDT. The SDT then voted between their preference as between Choice # 2 and Choice #3 and Choice #2 received greater than 2/3s of the members votes. The SDT agreed that the following should become 1.1:

> **1.1 *(Final)* Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.**

Criterion 1.2
- No changes

Criterion 1.3

"Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes."

SDT Comments before Polling
- Since Chicago the drafting team developed editorial changes.
- EEI suggested language "maintaining the stability and reliability of the BES."
- Does this refer to all units? Broad brush statement will confuse planning and coordination planners
- It needs to be more specific or it shouldn't be incorporated.
- Concept was to try to keep the idea in here.
- 12 units classified reliability must run up to 43 for Data Request Q3.
- Shutting down for security? No for reliability. They want to retire it and you'll require them to
- Go to R&R then goes to market. If it falls out of R&R, will shut down
- Unintended consequence may be a less reliable BES.
- This may work in a market but not in a non-market area. Have to be careful. Some language that- "retirement delayed" Auditors may ask, "Where is your study for every unit?"

Howard Gugel 9/28/10 4:49 PM
Comment: Not sure it is appropriate to include this

SDT Straw Poll on 1.3 As Written

Yes	***No***	***Abstain***	
13	**2**	**4=**	**68%**

Criterion 1.4
- No changes

Criterion 1.5:

"The Facilities comprising the Cranking Paths and initial switching requirements identified in the Transmission Operator's restoration plan."

SDT Straw Poll on 1.5 As Written

Yes	***No***	***Abstain***
11	**3**	**5=**

The SDT comments before polling touched on the following issues: seeking to get to the more the primary or initial cranking path; cranking path can be anything to get to any unit; data request indicated that 438 that will be identified as critical assets with 53 additional sub-stations; will this

bring in a disincentive to designate black start with multiple cranking paths; 1.5 and 1.9 taken together will bring in 627 transmission facilities + 250 generators as critical assets; concern every resource mentioned in operators restoration plan; does the current language enable a stop from 5 to 20 MW; and, generating facilities (keeping the turbine generator on and turning gear going) will have to come off of turning gear.

Following the poll, the SDT discussed: the problem with moving from low MW up to several higher levels; the term "facilities" is not specific to transmission or generation; the fact that 1.5 picks up from 1.4 and follows cranking paths till it reaches multiple path options. An ad hoc drafting group brought back the following language after a lunch break which the SDT agreed to:

> **1.5** *(Rewritten)***The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.**

SDT Straw Poll on 1.5 As Re-written

Yes	***No***	***Abstain***
16	**1**	**3**

The Chair agreed to review draft alternative language that Rich Kinas offered to develop. The following language was reviewed on Thursday by the SDT.

> **1.5 Alternative** *(Rich Kinas)* **"All facilities (transmission and generation) identified in the Transmission Operator's restoration required to start generation and re-establish a minimum of one synchronized tie with a neighbor."**

SDT Straw Poll on Alternative 1.5

Yes	***No***	***Abstain***
1	**17**	**0**

Criterion 1.7

"Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with four or more other stations."

SDT Comments

- There is a substantial drop in CA (70%) when at 4. Drop to 3.
- Dropping the phrase "or generating" addresses his issues.

Howard Gugel 9/28/10 5:18 PM
Comment: Who is his?

SDT Straw Poll

Yes	***No***	***Abstain***
17	**0**	**2**

Criterion 1.8

"Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Straw Poll

Yes	***No***	***Abstain***
17	**0**	**3**

Comments on 1.8

- Need to protect bus breakers on both ends of that line, i.e. at 2 stations not one. Take out "at a single station"?
- Without this we will have compliance issues, could have to deal with multiple locations. Don't believe the SDT has words on 1.8 right. Not going to violate an IROL. Jason Marshall will take a crack at different words for the SDT to consider.
- The Chair suggested we would come back to alternative language if it can improve its acceptability.

*Jason Marshall's alternative 1.8 language reviewed on 9-9. "***Transmission facilities that if destroyed, degraded, misused, or otherwise rendered unavailable, cause a reduction in an IROL magnitude or cause a new IROL to be identified."**

SDT Straw Poll

Yes	***No***
0	**18**

SDT Comments before the poll

- Do I have to evaluate all transmission facilities? That was why we had the language "at a single station location."
- How are TOP and planners to make these determinations? We may need examples for each of the key functions?
- We can go back to highlight resources we used initially in the drafting team in the guidance document. Works for ISOs.
- TOP and other transmission people may have trouble with this.

Criterion 1.9

"Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Comments

- No changes
- There were 0 assets on the survey.
- Intent to capture future- criticality for BES. If no purpose do we need this? Why called out? A: Because they have huge cyber systems which are easy to attack.
- **SDT Agreed to leave 1.9 in Attachment #1**

Criterion 1.10

"Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3."

SDT Straw Poll

Yes	*No*	*Abstain*
18	**0**	**3**

SDT Comments

- For criteria 9,10 and 12, "Misuse" different from the others
- "Misuse" –in order to cause a problem with the IROL. This is already covered.
- **SDT Agreed to leave 1.10 in Attachment #1**

Criterion 1.11

"Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements."

SDT Comments

- No changes
- This is a nuclear safety deal, vs. reliability issue.
- Tied to Nuc 001- in terms of safety.
- **SDT Agreed to leave 1.11 in Attachment #1**

Criterion 1.12

"Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs)."

SDT Comments

- Consistency editorial change by the Drafting Group.
- **SDT Agreed to leave 1.12 in Attachment #1.**

Criterion 1.13.

"Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes."

SDT Comments before polling

- The SDT found the NERC edits acceptable.
- "common"= shared?
- Language was taken out of Version 3.
- Because of the development of smart grid this is a bigger issue than it was in Version 1, 2 and 3.
- Put in 15 minute or real time. It is now pre-programmed into the device in the firm ware of the thermostat.
- This could be a problem without a time element.
- "Simultaneous" or "within a 15 minute period"?
- Issues with the smart grid are longer term. For this CIP 002-4 interim standard let's keep it simple.
- Used 15 minute in other criteria. "within 15 minutes"?
- "Under frequency" vs. "automatic" load shedding confusion. This doesn't apply to "manual load shedding."
- We may have a hard time in the future changing
- "designated for" vs. "responsible for."
- Used capable- due to compromise or misuse
- Is "capable through misuse" designated for automatic?
- Smart grid- distribution providers are out of scope? Going forward we will be better able to define it.
- Automatic load shed not manually initiated load shed.
- "Capability"- support keeping that concept in this criterion.
- "If misused could shed 300 mw or more within 15 minutes.
- Consider pulling automatic out- discrepancy between 2000 and 300 MK.
- The justification for 300MW is in DOE 317, Version 2.

Howard Gugel 9/28/10 5:21 PM
Comment: ??

SDT Straw Poll on 1.13 as written

Yes	***No***	***Abstain***
18	**2**	**0**

Comments after the rating

- Jim Bretton disagreed with putting time in.
- Bring in all DMS systems with removal of automatic if they have load-shedding capability.

- Rich Kinas noted this significantly changes the number of assets and prompts us to lose focus as to why we are here.
- Manual initiated operation- of cyber device- protection. EMS already considered.

Criterion 1.14

"Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator."

SDT Straw Poll

Yes	***No***	***Abstain***
16	**2**	**2**

Comments before Polling

- The drafting team and NERC offered only editorial changes.
-
- Should we drop this one?
- Control systems in 1.14.
- If combined we don't have a criteria of 2300 MW. Will be covering a lot of entities without the bright line.
- New advanced persistent threats at layer 7 at application layers are a concern. These are not being picked up by firewalls. Understand this creates a burden on these small entities but they and we need protection at the same level. Size doesn't matter when it comes to attack vectors.
- Control systems need to be protected.
- On control center criteria- don't understand survey results and why it didn't result in dropping a lot off the list? How did we lose 5 RCs? While these are close enough they are not reliable data figures and need more analysis.
- "Connectivity and size doesn't matter." IP is everything and everywhere. Controls should be inadequate for the control system. Can't buy the argument that connectivity is all that matters.
- Look at just this standard. If you put them all in it will be a huge impact. Can't solve all the problems with this standard.
- Consider changing "every" to "each"?
- Can't afford to ignore. Can't imagine that FERC would allow us to get away with 2300. It is there and it is a vulnerability.
- We are mixing 1.14 and 1.15 in our discussion. Threshold for control generation- control centers = 2 of more physical assets.
- Entities as GOPs are designating. GOP in 1.14?
- That is an "or" in 1.15.
- Can't worry about connectivity. Worried about letting it come into language. Some GOPs have control centers controlling few MW and 1 or 2 plants.

Howard Gugel 9/28/10 5:22 PM
Comment: Does not pertain to this language

Howard Gugel 9/28/10 5:23 PM
Comment: Not sure what this means.

Howard Gugel 9/28/10 5:25 PM
Comment: Not sure of context

Howard Gugel 9/28/10 5:26 PM
Comment: Context?

Howard Gugel 9/28/10 5:26 PM
Comment: What does this mean?

- 1.14 is based on EOP 008 which doesn't include GOP.
- We don't have a definition of control centers in 002-4.
- 1.14- can't rely on EOP 008- not required to have a back up control center. Lots of ways of meeting standards. It may be problematic to call this out as a reason.
- This is because we don't have concrete definition for control center. Focus on the control systems.
- Back up control centers- doesn't say you have to have a back up center, but if you do you must secure.
- EOP 008 doesn't have qualifications so we don't need them either. We need a justification.
- EOP 008 not referenced in the guidance.

Criterion 1.15:
"Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 2300 MWs in a single Interconnection."

SDT Straw Poll on 1.15 as presented.

Yes	*No*	*Abstain*	
15	**2**	**2=**	**79%**

The SDT discussed the criterion which links back to 1.1 and discussed it as presented and identified the following concerns: this will probably get this sent back from FERC; need to clarify why 1.1 uses 2000 MW and this uses 2300 MW; should "control systems" be added to be consistent with 1.15; there may be control systems that are computerized but that are not connected; control centers appear in CIP versions 1, 2 & 3 so removing the focus on control centers would need to be justified; this is a transition to a function focus of CIP 010 & 011; control room vs. control center doesn't have to be analyzed separately from asset it controls; control centers operated by generation operators with no transmission but just control and dispatch; what about renewables or variable generation; and what does control generation mean? 1.15: centers being used to control generation- don't control breakers, just establishing a set point. Easy for it to be taken off until they are sure it is the right signal they should be following. 2300 explanation good break point.

Howard Gugel 9/28/10 5:27 PM
Comment: Should this be in here?

SDT Straw Poll- delete "in a single interconnection"

Yes	*No*	*Abstain*	
6	**12**	**1=**	**32%**

Criterion 1.16
"Any facility declared by a regulatory agency to be critical to national security."

Howard Gugel presented the criterion that was not proposed by the SDT CIP 002-4 drafting team but proposed by NERC staff. He noted the NERC data request showed that only 17 nuclear generation facilities are included in the existing risk-based methodology. If nuclear generation is added as a specific criterion, that number rises to 88. The SDT reviewed the statement noting the following concerns: this is a overbroad statement and a back handed way to get nuclear in; NERC is a reliability

Howard Gugel 9/28/10 5:29 PM
Comment: Not sure this should be a matter of record

organization and the SDT is working on a reliability standard; other regulators have their own processes, this doesn't belong here; there are 57 bills in the U.S. Congress giving power to the President and others to declare emergency, but until the industry get these directives from Congress and then FERC and NERC it is premature to address.

The SDT unanimously decided not to include this criterion statement in Attachment 1.

Criterion 1.17
"Any additional assets that the Responsible Entity deems appropriate to use."

The SDT discussed adding this statement back into Attachment 1 that had been removed in Chicago. The NERC data request shows 307 critical assets would be identified under this criteria. While this may be primarily an optics issues there would be no down side and it might help fund some security investment.

Howard Gugel 9/28/10 5:34 PM
Comment: Not sure the discussion considered funding. It revolved arould justifying existing Critical Asset methodology that captured assets not identified in the new criteria.

SDT Straw Poll

Yes	***No***	***Abstain***
17	**3**	**0**

Nuclear Generation Criterion

John Lim noted that the NERC president, Gerry Cauley, met with EEI executives who agreed that it would be a prudent thing to add nuclear generation as a critical asset criterion. Given the timing, the Chair proposed that members consult with their management to get additional feedback and that this issue would be up for review and possible adoption by the SDT at its September 15 conference call. It was noted that lowering 1.1 to 1500 MW will bring in more nuclear generation facilities.

A motion to adopt Attachment 1 as revised was offered by Sharron Edwards and seconded by Doug Johnson.

SDT Member Vote on Attachment #1 as Revised

Yes	**No**	
18	**1=**	**95%**

Jim Brenton voted no and offered the following explanation of his vote. "Draft CIP 002 Version 4, Attachment 1, does not require that nuclear generation plants be designated as Critical Assets per CIP-002-4. Generation Operator Control Centers and Control Systems are not designated as Critical Assets per Draft CIP 002 Version 4, Attachment 1. Many of these facilities are interconnected via real time network connections and cyber security exploits at

the application level can transverse between trusted nodes only protected at Layer 4 (firewalls and Router ACL). An insufficient number of Generation Units will be designated as Critical

Assets with the criteria in Attachment 1, Criterion 1.1 set at 1500 MW. The draft CIP 002 Version 4, Attachment 1 language related to IROLs is vague and will cause problems for TOP, TP and other registered entities in making CA determinations—it is not a bright line or a deterministic metric—since the values may change dynamically. I generally support the language provided. However, the team had an opportunity but failed to address the nuclear generation issue and the need for including sufficient generation facilities under the proposed standards, both of which I consider show stoppers, as I articulated to all during the meeting.

Howard Gugel, NERC staff, noted he would check with NERC management but that he agrees with the SDT's approach to delay the vote until members can check with their management team. If, however, the SDT agreed to post without nuclear generation included as critical assets in it, the public document posting will occur in the middle of election season in the U.S.

Howard Gugel 9/28/10 5:36 PM
Comment: I do not believe that I stated that I agreed with the approach to not include nuclear.

D. CIP -002-4 Implementation Plan

Following the Chicago meeting, SDT member Dave Revill led a lead a team (Sharon Edwards, Phil Huff, Dave Norton, Scott Rosenberg, and Kevin Sherlin. Mike Keane FERC and Scott Mix NERC, Joe Bucciero, facilitator) to develop a new draft of the implementation plan based on the Chicago input. It was presented to the SDT on the August 26 conference call. He noted the proposed sliding 18 month window for new assets not identified in the first application that are identified as a result of an update ("update as necessary") during the first 12 months. This in effect meant entities may have anywhere from 12 to 30 months to be compliant. R2 locks in which cyber assets we are talking about and those "critical cyber assets "associated with" critical assets newly identified by CIP 002-4.

The SDT discussed regarding the proposal including: confusion between FERC approval vs. effective date; given the doubling the generation and transmission facilities in scope (not Version 2 and 3 didn't anticipate the doubling of assets) 18 months is not that long a time; if we can't meet schedules because vendors are not ably to supply we must self report unless there is an exception process; if newly identified asset or control entity that hasn't dealt with before -24 months; in accelerating schedule for few requirements we have made this more complicated without really gaining much; we will also be introducing concept of CIP 010 and 011 during same period; consider a phased approach given the number of assets that need to be addressed; can regional entities deal with an exceptions process; if we just make it 24 months across the board then simplify some of these exceptions; and the regulator perspective may be that 18 months is too long a timeframe.

Following the discussion the drafting group met over lunch and came back with a proposal for a timeline which intended to provide an 18 month plus 6 months window and removed the 12 month window and made it instead a separate exception. They noted that they were not recommending an exception process because of the challenge in standing it up for this interim standards with the appropriate oversight, change the NERC rules of procedure and difficulty of implementing at the regional level. From 2006-2009 the industry identified over 4500 critical assets in 3 years with no

previous experience. This proposal would add around another 2000 critical assets (or an additional 50%) in two years. This could also be part of the feedback from the industry in the comment form.

The SDT and participants discussed the proposal offering the following points and concerns: just because it would be hard to create an exception process, doesn't justify setting the industry up for failure; power plants are very different and more complex than substations; Q 1.2 responses from the NERC data request suggests about 370 generation or a 93% increase nearly doubling existing numbers; this generation asset doubling may provide justification for the 24 vs. 18 months; version 1-FERC 706 beginning of 2008 was in essence a 24 month implementation plan; the implementation timeline for nuclear assets is 2 years with allowance for outages; though each Province varies, in general, NERC standards for Canadian entities are effective upon NERC board approval, however the effective implementation takes place upon FERC approval; should generation assets get 24 months and all others 18 months.

The SDT then polled the following implementation timeline:

Implementation Timeline- Overall 24 months (6 months for identification of critical assets and 18 months for critical assets in compliance)

Straw Poll on Timeline

Yes	No	Abstain
18	**0**	**0**

Motion to Approve the Implementation Plan as Revised with friendly amendments *("18 months after effective date") (See Appendix #)* Dave Revill with Sharon Edwards 2nd.

Yes	*No*
18	**0**

E. CIP 002-4 Reference (Guidance) Document

The Reference Document (formerly "guidance document") was initially reviewed at the August 26 SDT conference call and on Wednesday afternoon. On Thursday afternoon the SDT reviewed the reference document noting that there will be conforming edits based on the agreements reached by the SDT on CIP 002-4 and Attachment 1 and on the implementation plan. The SDT and participant discussion of the document included the following points: put some of the survey results into the guidance document supporting how this is protecting the public; use "reliable operation" which is from the standard vs. the terms "reliability or operability"; change facilities to "designated as a facility"; stay away from the term control room/facilities; guidance for CIP 2 1-3.Where does that guidance fit relative to CIP 4? Is it going away, should be considered and mentioned; critical asset identificaiton guideline becomes largely irrelevant because of the removal of the risk based approach; Critical Assset identification guidelines are still relevant; John did a good job explaining without

expanding; take out the "one button" in the rationale for 1.13 to avoid confusion with automatic load shedding."

Following the SDT review and discussion Sharon Edwards made a motion to accept the Reference Document as revised and David Revill seconded the motion with the proviso that this will be brought back to the SDT conference call on September 15 for final adoption.

Yes	No	Abstain
18	0	1

F. VSLs/VRFs

Howard Gugel reported on the draft VSLs and VRFs. He noted in the interest of minimal changes, the subR format is still being used here.

Howard Gugel 9/28/10 5:40 PM
Comment: These were not reviewed in Chicago

Members offered the following points in the review of the draft VSLs: add R2- "performing a function essential"; delete "list" and "as per requirement after operation of the Critical Asset; consider changing to bullets; consider rolling up the SubRs under severe R2; and, without an exception process as discussed yesterday in the implementation plan, how many in violation when entity did a self-reporting.

Members offered the following points in the review of the draft VRS; keep these as separate sub Rs on this table because they have different impact levels; is it a double jeopardy issue if you are in violation of a lower and a high when you have separate Sub Rs; when you have a high level requirement R2 that has a VRF with it and the Sub Rs have vrfs are at a lower level, if there is a violation of 2.1 is it also a violation of R2; auditors can't discuss VRF and VRS, they simply find a violation and findings on an audit are always rolled up to the highest level; then it becomes an enforcement issue determined by an enforcement team at a sub component; there are many requirements wrapped into R2; take the definitional parts and have as bullet points.

The SDT unanimously approved the VSL and VRS documents as revised.

G. Cover Letter and Comment Form

Howard Gugel reviewed with the SDT a draft Cover Letter and Comment form. The Vice Chair drafted and the SDT agreed to add two paragraphs that referenced the CIP 010 and 011 development and its relation to the CIP 002-4. Howard clarified that the CIP 003-009 version 4 package would be posted with CIP 002-4 with conforming references and applicability section changes. It was suggested that VSLs and VRFs be referenced as 2 separate questions.

Doug Johnson made a motion and Jay Cribb seconded to adopt the Cover Letter and Comment Form as revised for posting with CIP 002-4.

Yes	No
19	0

H. Preparation for CIP 002-4 September 29, 2010 Webinar

The SDT reviewed a draft agenda and proposed assignments for an industry webinar on September 29 from 11:00 a.m. -1 p.m. on the CIP 002-4 filing, which the Chair outlined. Allen Mosher, Chair of the NERC Standards Committee will provide some introductory remarks in terms of the context and recent history of the SDT's efforts. It was noted that the presentations would be at a relatively high level with the intention of leaving sufficient time of the Webinar devoted to Q & A. There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard.

There will also be a short presentation by an industry representative member of the CIP 005 urgent action work group on the substance and procedure for that draft standard. It was agreed that a power point template would be circulated and a dry run will take place on September 20 with the slides to NERC by September 22.

III. PROGRESS REPORT ON CIP FRAMEWORK SUB-TEAM

Dave Norton, Sub-Team lead, reported on the two meetings the Framework Sub-Team has convened (See, Appendix 8). He suggested the context is that some in the industry stakeholders did not like what they saw with CIP-011, and the regulator doesn't think we have approached things consistently with the NIST 800-53 framework, thereby establishing a baseline at the outset. The Sub-Team has agreed that the SDT needs to answer the question, "what are we protecting and from who?" There are threats, vulnerabilities and impacts to consider but threats are hard to be clear on, and impacts have a lot of permutations. The Sub-Team is initially focusing on known vulnerabilities in the open information sources and posing the question: how can we use known vulnerabilities to link to specific standards (e.g., NIST IR volume 3, Chapter 7 treatment of vulnerabilities). The original CIP standard team learned that it is very difficult to write CIP requirements that address the old and new at the same time, resulting in overkill for the old and leaving modern vulnerabilities unaddressed. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework for the CIP standards, and not a format. Ultimately this should lead to a format.

The Sub-team is currently pulling nuggets out from others have done before. The output should be a justification and rationale underpinning the standards, not the standards themselves. They are starting with a framework not a format. Ultimately this should lead to a format.

Dave Revill noted that when the SDT developed CIP-011, we identified requirements at the high impact level and forced the scoping elements on them. The Framework Sub-Team's idea is to start from the bottom and work up.

Member and Participant Comments

- Think about differences between serial line with an operating system vs. embedded software systems on serial lines. Different vulnerabilities. We have to think of the differences- need people who understand on how the code works.
- CIP 11 security controls lacked a basis to come back to what the measure of success was.
- We should identify threats and ask is it "appropriate" based on operating environment and the characteristics of the device.
- As a model of identifying a baseline and incorporating appropriate NIST features, can you get there without dealing with the issue with the present compliance model? If no reward system in addition to the punitive system of compliance will this work?
- As far as possible, it will be advantageous to maintain the current structure and modify a bit, then we can be responsive to that faction in the ballot pool.
- What ever appears to work will come naturally if we start at what are we trying to protect and let the structure come to that.
- E.g. on format, big middle and little. Impact classes of assets within each a category of cyber assets?
- Acknowledge the differences between a generation vs. transmission mindset.
- Agree on the "appropriate" mantra, but need to pin down what this means. Have to drill down.
- The model that we have may be ok. The implementation of the model (over zealousness of some of the audit staff and unevenness of the quality) is where the problem arises. The industry is not complaining about audits, but about the process as implemented that is not true to standards and fair and equitable across the regions.
- The Sub-teams hope is that they can get to more granular statements that are specific to technology so we can minimize TFEs.
- VRF/VSLs- 0 tolerance is problem for compliance. Gradual incremental improvement.
- From NERC and FERC the view is that self-reports are a good thing or at least a better thing than hiding it. Industry executives don't view it that way.
- FERC is looking for the industry to define what appropriate is. It doesn't mean none, has to meet some rational tests.
- In a compliance based standard context, lawyers and management see it differently from those who are trying to fix things and make them more secure. Impossible to write a standard that covers everything. FERC order 693 requires audit to the requirements.
- The Sub-team will be reviewing again what exactly does 706 say to do.

The Chair noted that the Framework Sub-Team will have a significant amount of agenda time during the Toronto SDT Meeting in October to bring the SDT up to date and engage them in discussion of the key issues. These discussions should provide guidance as the Sub-Team continues its efforts to bring back a framework that the SDT can review, refine, and adopt at its December 2010 meeting that will guide its work in 2011.

IV. NEXT STEPS AND ASSIGNMENTS

On Friday morning the SDT reviewed the progress being made by the CIP 010 and 011 sub-teams in summarizing industry responses and the Dallas workshop comments. The Chair thanked those sub-groups who had completed their tasks and asked all the sub-groups to complete their summaries by the SDT October meeting

The Team reviewed the preparations for the CIP 002-4 Webinar *(see Section II. H above)* which will take place on September 29 from 11:00 a.m.- 1:00 p.m.

The Chair reviewed the schedule for a SDT conference call meeting on Wednesday, September 15 from 10:00 a.m.-12:00 p.m. (eastern time) to review the final documents for posting that were not adopted at this meeting and to determine whether the SDT members, following review with their corporate senior management, wanted to revisit the SDT's previous decisions on whether to specifically include all nuclear generation as a criterion for assessment in CIP-002-4 Attachment 1.

The Toronto agenda was discussed and SDT member and host Rob Antonishen described the Toronto, Ontario venue for the meeting.

The meeting adjourned at 9:45 a.m. on Friday, September 10.

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 26th Meeting Agenda
September 8, 2010, Wednesday- 8:00 AM to 6:00 PM CDT
September 9, 2010 Thursday- 8:00 AM to 6:00 PM CDT
September 14, 2010 Friday- 8:00 AM to 10:00 AM CDT
Manitoba Hydro Place
360 Portage Ave., Winnipeg, Manitoba, Canada

NOTE: 1. Agenda Times May be Adjusted as Needed during the Meeting
NOTE: 2. Drafting Sub-team Meetings May Not Have Access to Telephones and Ready Talk

Proposed Meeting Objectives/Outcomes:

- To review, clarify, refine and adopt the draft CIP-002-4 standard, Implementation Plan and Guidance Document for posting
- To review and discuss the implications of the NERC Mandatory Data Request results for the CIP 002-4 draft
- To review agenda and assignments for CIP-002-4 September 29 Webinar
- To review progress of the Frameworks Sub-team, and the sub-teams draft responses to industry and Dallas workshop comments
- To agree on next steps and assignments

Wednesday, September 8, 2010 8:00 a.m. - 6:00 p.m.

- Introduction, welcome, and opening and guest remarks -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review NERC comments on draft CIP-002-4 standard *(Morning)*
- Review and refine draft CIP 002-4 standard and related documents (including CIP-002-4, VSL/VRFs, Implementation Plan, Guidance document for CIP 002-4) *(Morning)*
- Review of NERC Data Request responses for consideration in CIP-002-4 Attachment #1 Criteria *(Afternoon)*

Thursday, September 9, 2010 8:00 a.m. - 6:00 p.m.

- Finalize draft of CIP 002-4 standard *(Morning)*
- Discuss related documents (including VSL/VRFs, Implementation Plan, and Guidance document for CIP 002-4, Comment Form, Cover Letter) *(Morning and Afternoon)*
- Adoption of CIP 002-4 documents for posting *(Afternoon)*
- Review Summary Response Documents for Attachment 2, CIP-010 *(Afternoon & Evening)*

Friday, September 10, 2010, 8:00 a.m. - 10:00 a.m.

- Review Preparation for CIP 002-4 September 29 Webinar *(Morning)*
- Review Progress report on CIP Framework sub-team (*Morning)*
- Review progress reports on Sub-teams' draft summaries of industry and Dallas workshop comments
- Review SDT October12-14, 2010 Toronto Meeting Agenda (*Morning)*

Appendix # 2 Attendees List
September 8-10, 2010 Winnipeg

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jim Brenton	ERCOT
3. Jackie Collett	Manitoba Hydro
4. Jay S. Cribb	Southern Company Services
5.Joe Doetzl	Kansas City Pwr. & Light Co
6. Sharon Edwards	Duke Energy
7.Gerald S. Freese	America Electric Pwr.
8. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
9. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation
10. Doug Johnson	Exelon Corporation – Commonwealth Edison
11. John Lim, Chair	Consolidated Edison Co. NY
12. David Norton	Entergy
13. David S. Revill	Georgia Transmission Corporation
14. Tom Stevenson	Constellation
15. Keith Stouffer	National Institute of Standards & Technology

SDT Members Attending via ReadyTalk and Phone

16. Scott Rosenberger	Luminant Energy (W/Th)
17.Rich Kinas	Orlando Utilities Commission (W/Th)
18. John D. Varnell	Technology Director, Tenaska Power Services Co. (W/Th)
19. John Van Boxtel	WECC (W)
20 William Winters	Arizona Public Service, Inc. (W/Th)
21.William Gross	Nuclear Energy Institute (W/Th)
22.Kevin Sherlin	Sacramento Municipal Utility District (Th)
Scott Mix	*NERC*
Howard Gugel	*NERC*
Brian Harrell	*NERC*
Roger Lampila	*NERC*
Joe Bucciero	*NERC/Bucciero Consulting, LLC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

Howard Gugel 9/28/10 5:42 PM
Comment: I do not think these entries belong in this table. We were in person, not on ReadyTalk

SDT Members Not Participating

Patricio Leon	Southern California Edison
Jonathan Stanford	Bonneville Power Administration

Others Attending in Person

Justin Kelly	FERC
Greg Fraser	G.J. Fraser Consulting
Joel Garmen	Next Era Energy (FPL) (T/W/Th)
Robert Preston Lloyd	Southern California Edison
Michael Keane	FERC
Nathan Mitchell	APPA
Brian Newell	American Electric Power
Mark Simon	Encari
Tom Alrich	Matrikon
Guy Zito	NPCC (T/W)

Howard Gugel 9/28/10 5:57 PM
Comment: Allen did not attend this meeting

Others Attending via Readytalk and Phone

September 8, 2010, Wednesday

Bryn	Wilson	wilsonwb@oge.com
andres	Lopez	andres.lopez@usace.army.mil
Roger	Fradenburgh	rfradenburgh@netsectech.com
Amir	Hammad	amir.hammad@constellation.com
jan	Bargen	jan.bargen@ferc.gov
Monte	Moorehead	mpmoorehead@midamerican.com
matt	Jastram	matt.jastram@pgn.com
Robert	Ford	robert.w.ford@usace.army.mil
David	Batz	dbatz@eei.org
Jason	Marshall	jmarshall@midwestiso.org
Patricia	Lynch	patricia.lynch@nrgenergy.com
Larry	Camm	larry_camm@selgs.com
Tom	Alrich	tom.alrich@matrikon.com
Bob	Case	Bob.Case@blackhillscorp.com
Rod	Hardiman	rchardim@southernco.com
Vincent	Le	vincent.le@ferc.gov
Maggy	Powell	margaret.powell@constellation.com
Russell	Noble	rnoble@cowlitzpud.org
Annette	Johnston	AJJohnston@midamerican.com
Drew	Kittey	Drew.Kittey@ferc.gov
David	Gordon	dgordon@mmwec.org

Al	Mendoza	patricio.leon-alvarado@sce.com
Roger	Fradenburgh	rfradenburgh@netsectech.com
Ingrid	Rayo	ingrid.rayo@constellation.com
Sharla	Artz	sharla_artz@selgs.com

September 9, 2010, Thurssday

Bob	Case	Bob.Case@blackhillscorp.com
Russell	Noble	rnoble@cowlitzpud.org
Jan	Bargen	jan.bargen@ferc.gov
Stephen	Thomas	Stephen.J.Thomas@constellation.com
Bill	Keagle	william.a.keagle.jr!@bge.com
Rod	Hardiman	rchardim@southernco.com
Sharla	Artz	sharla_artz@selgs.com
David	Gordon	dgordon@mmwec.org
Larry	Camm	larry_camm@selgs.com
Dave	Batz	dbatz@eei.org
Tom	Alrich	tom.alrich@matrikon.com
Vincent	Le	vincent.le@ferc.gov
Drew	Kittey	Drew.Kittey@ferc.gov
Jason	Marshall	jmarshall@midwestiso.org
Robert	Ford	robert.w.ford@usace.army.mil
Ingrid	Rayo	ingrid.rayo@constellation.com
Bryn	Wilson	wilsonwb@oge.com

September 10, 2010, Friday

Larry	Camm	larry_camm@selgs.com
Bill	Keagle	william.a.keagle.jr@bge.com
Ingrid	Rayo	ingrid.rayo@constellation.com
Sharla	Artz	sharla_artz@selgs.com
Tom	Alrich	tom.alrich@matrikon.com
Rod	Hardiman	rchardim@southernco.com
jan	bargen	jan.bargen@ferc.gov
Bryn	Wilson	wilsonwb@oge.com
Russell	Noble	rnoble@cowlitzpud.org

Appendix #3 NERC Antitrust Compliance Guidelines

See Antitrust Compliance Guidelines read at the beginning of each day's session at:

(NEED LINK)

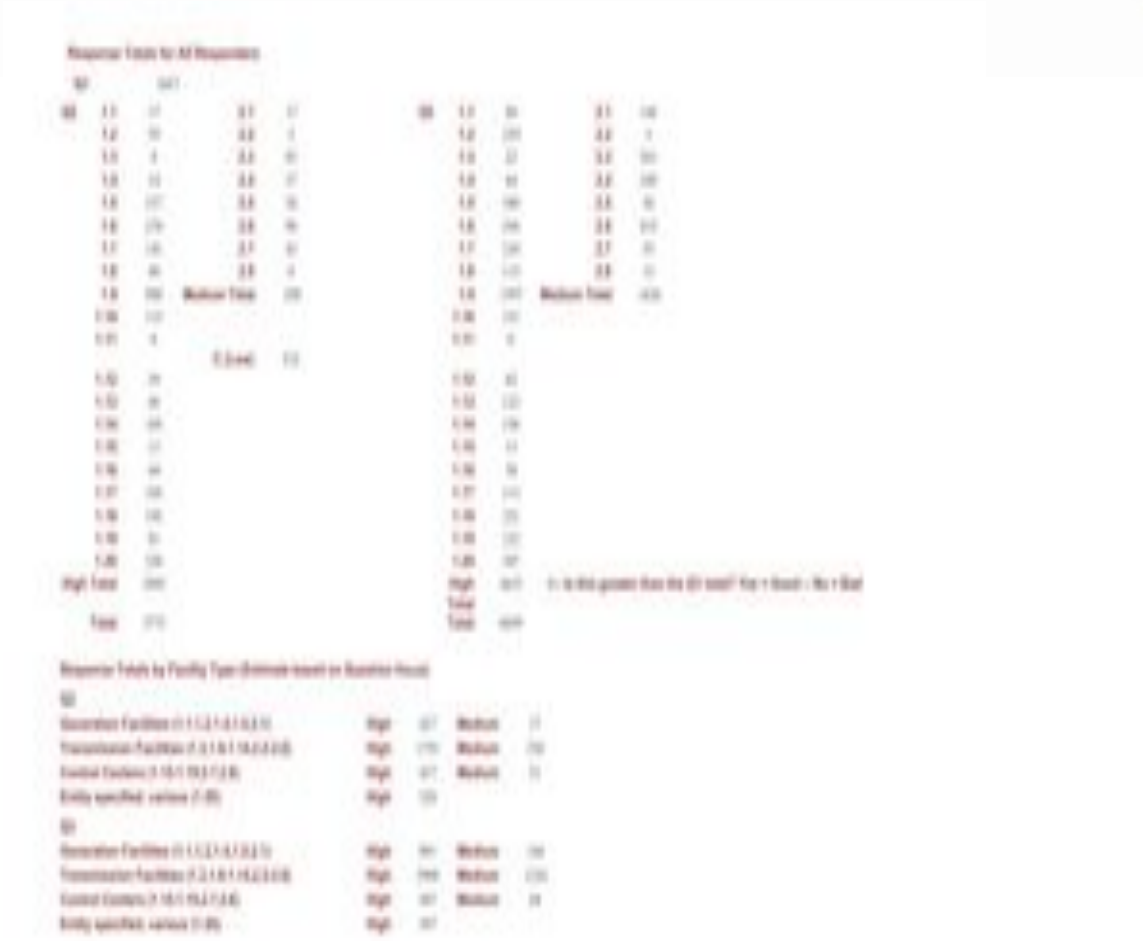
The NERC reminder below was read at the beginning of each day's session.

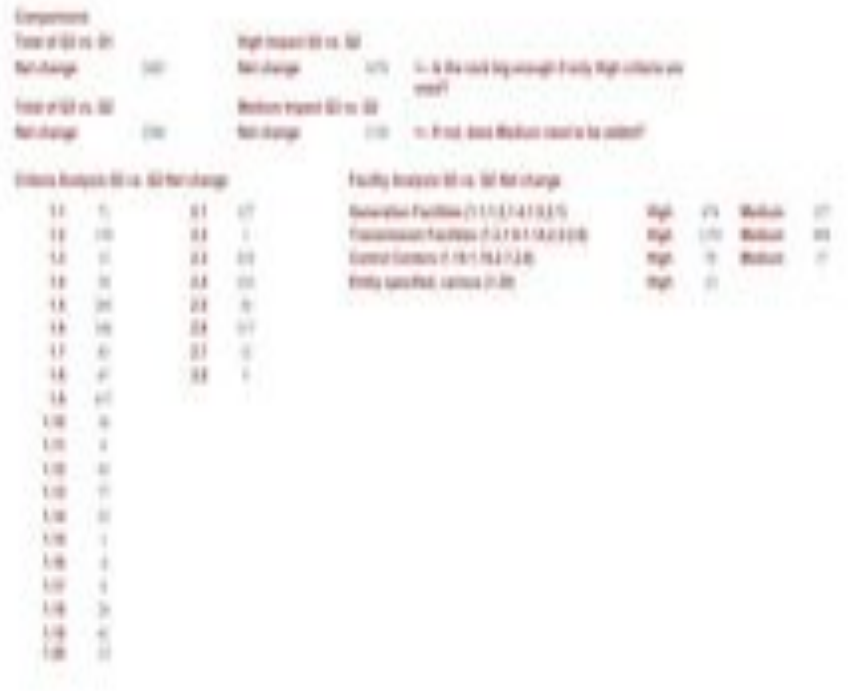
NERC REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Appendix # 4- Raw Results- NERC Data Request





Appendix # 5- CIP 002-4 Adopted Draft (9-9-10)

Introduction

1. **Title:** Cyber Security — Critical Cyber Asset Identification

2. **Number:** CIP-002-4

3. **Purpose:** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

   These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

   Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

   Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

4. **Applicability:**

   4.1. Within the text of Standard CIP-002-4, "Responsible Entity" shall mean:

   4.1.1 Reliability Coordinator.

   4.1.2 Balancing Authority.

   4.1.3 Interchange Authority.

   4.1.4 Transmission Service Provider.

   4.1.5 Transmission Owner.

   4.1.6 Transmission Operator.

   4.1.7 Generator Owner.

   4.1.8 Generator Operator.

   4.1.9 Load Serving Entity.

   4.1.10 NERC.

4.1.11 Regional Entity.

4.2. The following are exempt from Standard CIP-002-4:

4.2.1 Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

5. **Effective Date:** The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)

Requirements

R1. Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment I – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

R2. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R2.1 The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
R2.2 The Cyber Asset uses a routable protocol within a control center; or,
R2.3 The Cyber Asset is dial-up accessible.

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

Measures

M1. The Responsible Entity shall make available its list of Critical Assets as specified in Requirement R1.

M2. The Responsible Entity shall make available its list of Critical Cyber Assets as specified in Requirement R2.

M3. The Responsible Entity shall make available its approval records of annual approvals as specified in Requirement R3.

Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority

1.1.1 Regional Entity for Responsible Entities that do not perform delegated tasks for their Regional Entity.

1.1.2 ERO for Regional Entity.

1.1.3 Third-party monitor without vested interest in the outcome for NERC.

1.2. Compliance Monitoring Period and Reset Time Frame

Not applicable.

1.3. Compliance Monitoring and Enforcement Processes

Compliance Audits

Self-Certifications

Spot Checking

Compliance Violation Investigations

Self-Reporting

Complaints

1.4. Data Retention

1.4.1 The Responsible Entity shall keep documentation required by Standard CIP-002-4 from the previous full calendar year unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

1.4.2 The Compliance Enforcement Authority in conjunction with the Registered Entity shall keep the last audit records and all requested and submitted subsequent audit records.

1.5. Additional Compliance Information

1.5.1 None.

2. Violation Severity Levels (To be developed later.)

Regional Variances

None identified.

VERSION HISTORY

Version	Date	Action	Change Tracking
1	January 16, 2006	R3.2 — Change "Control Center" to "control center"	03/24/06
2		Modifications to clarify the requirements and to bring the compliance elements into conformance with the latest guidelines for developing compliance elements of standards. Removal of reasonable business judgment. Replaced the RRO with the RE as a responsible entity. Rewording of Effective Date. Changed compliance monitor to Compliance Enforcement Authority.	
3		Updated version number from -2 to -3	
3	12/16/09	Approved by the NERC Board of Trustees	Update
4	09/20/10	Modified to provide bright-line criteria for the identification of Critical Assets.	

CIP-002-4 - Attachment I

CRITICAL ASSET CRITERIA

The following are considered Critical Assets:

1.1. Each group of generating units (including nuclear generation) at a single plant location with an aggregate highest rated net Real Power capability of the preceding 12 months equal to or exceeding 1500 MW.

1.2. Each reactive resource or group of resources at a single location (excluding generation Facilities) having aggregate net Reactive Power nameplate rating of 1000 MVARs or greater.

1.3. Each generation Facility that the Planning Coordinator or Transmission Planner designates as required for reliability purposes.

1.4. Each Blackstart Resource identified in the Transmission Operator's restoration plan.

1.5. The Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan up to the point on the Cranking Path where multiple path options exist.

1.6. Transmission Facilities operated at 500 kV or higher.

1.7. Transmission Facilities operated at 300 kV or higher at stations interconnected at 300 kV or higher with three or more other transmission stations.

1.8. Transmission Facilities at a single station location that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.9. Flexible AC Transmission Systems (FACTS) at a single station location, that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.10. Transmission Facilities providing the generation interconnection required to directly connect generator output to the transmission system that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of the assets described in Attachment 1, criterion 1.1 or 1.3.

1.11. Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements.

1.12. Each Special Protection System (SPS), Remedial Action Scheme (RAS) or automated switching system that operates BES Elements that, if destroyed, degraded, misused or otherwise rendered unavailable, violate one or more Interconnection Reliability Operating Limits (IROLs).

1.13. Common control system(s) capable of performing automatic load shedding of 300 MW or more within 15 minutes.

1.14. Each control center, control system, backup control center, or backup control system used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator.

1.15. Each control center or backup control center used to control generation identified as a Critical Asset, or used to control generation greater than an aggregate of 1500 MWs in a single Interconnection.

1.16. Any additional assets that the Responsible Entity deems appropriate to include.

CIP-002-4	R1.	Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in CIP-002-4 Attachment 1 – Critical Asset Criteria. The Responsible Entity shall review this list at least annually, and update it as necessary.	N/A	N/A	The Re Entity h develop Critical the list been re updatec as requ	
CIP-002-4	R2.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	N/A	N/A	The Re Entity h develop associa Cyber A perform functio to the o the Crit but the been re updatec as requ	

CIP-002-4	R2.1	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	N/A	N/A	N/A	
CIP-002-4	R2.2.	The Cyber Asset uses a routable protocol within a control center; or,	N/A	N/A	N/A	
CIP-002-4	R2.3.	The Cyber Asset is dial-up accessible.	N/A	N/A	N/A	
CIP-002-4	R3.	Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2, the Responsible Entity may	N/A	N/A	The Re Entity have a dated r senior delegat	

		determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)			annual the list Assets. OR The Re Entity have a dated re senior delegat annual the list Cyber (even i are null	

Appendix #6 Implementation Plan (Final)

Implementation Plan for Version 4 of

Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before this standard can be implemented.

Applicable Standards

The following standards are covered by this Implementation Plan:
CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 —Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

These standards are posted for ballot by NERC together with this Implementation Plan. When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4

Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard.

Proposed Effective Date for CIP-003-4 – CIP-009-4

Critical Cyber Assets Already in Compliance with CIP-003-3 – CIP-009-3

Critical Cyber Assets identified by CIP-002-4 R2 that are already compliant with CIP-003-3 through CIP-009-3 shall be compliant with the requirements of CIP-003-4 through CIP-009-4 on the Effective Date specified in each version 4 Standard.

Critical Cyber Assets Associated with Critical Assets Newly Identified by CIP-002-4

U.S. Nuclear Power Plant Facilities

For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 by the latter of (i) 18 months after the Effective Date of CIP-002-4 or (ii) 6 months following the completion of the first refueling outage beyond 18 months from the Effective Date of CIP-002-4 for those requirements requiring a refueling outage.

All Facilities Other Than U.S. Nuclear Power Plant Facilities

For Responsible Entities who previously identified Critical Cyber Assets under CIP-002-1 R3, CIP-002-2 R3, or CIP-002-3 R3; Critical Cyber Assets associated with Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4.

All Other Critical Cyber Assets

For all cases not identified above, Critical Cyber Assets shall be compliant with the requirements of **CIP-003-4 through CIP-009-4** by the latter of (i) the Effective Date specified in each Version 4 Standard or (ii) the compliance milestones in the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* based on the earliest date of identification of the Critical Cyber Asset from CIP-002-1 R3, CIP-002-2 R3, CIP-002-3 R3, or CIP-002-4 R2.

Implementation Plan for Newly Identified Critical Cyber Assets and

Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible

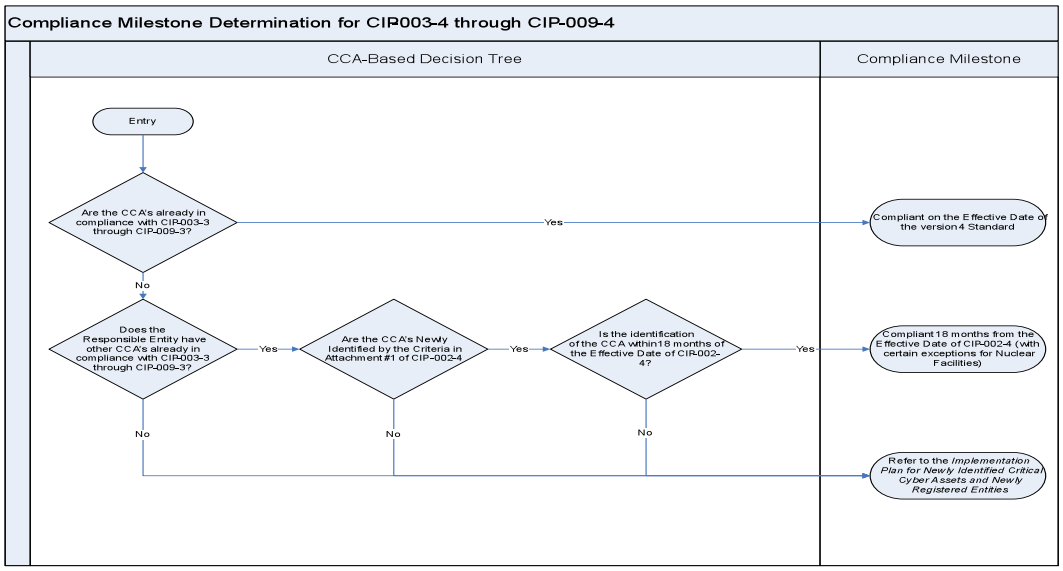
Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation Plan would apply based on the situations identified in the above section, *Proposed Effective Date*. This Implementation Plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.

The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

Prior Version Standard Retirement

Standards CIP-002-3 – CIP-009-3 shall be retired upon the Effective Date of the corresponding Version 4 Standard.



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Appendix #7 Letter and Comment Form

September 20, 2010

TO: INDUSTRY STAKEHOLDERS

RE: **REQUEST FOR COMMENTS REGARDING THE DRAFT OF CIP-002-4 THROUGH CIP-009-4**

Ladies and Gentlemen:

In 2008, FERC Order 706 paragraph 236 directed the ERO to develop modifications to Standard CIP-002-1 Cyber Security – Critical Cyber Asset Identification to address their concerns regarding: (1) the need for ERO guidance regarding the risk-based assessment methodology; (2) the scope of critical assets and critical cyber assets; (3) internal, management approval of the risk-based assessment; (4) external review of critical assets identification; and (5) interdependency analysis.

A Standards Drafting Team (SDT) was appointed by the NERC Standards Committee on August 7, 2008 to develop these modifications as part of Project 2008-06 – Cyber Security Order 706. The SDT has been charged to review each of the CIP reliability standards and address the modifications identified in the FERC Order 706. The SDT began meeting in October 2008.

Prior to this posting, the SDT developed CIP-002-2 through CIP-009-2 to comply with the near-term specific directives of FERC Order 706. This version of the Standards was approved by FERC in September of 2009 with additional directives to be addressed within 90 days of the order. In response, the SDT developed CIP-003-3 through CIP-009-3, which FERC approved in March 2010.

Throughout this period, the SDT has continued efforts to develop an approach to address the remaining FERC Order 706 directives. Most recently, CIP-010 and CIP-011were posted for informal comment in May of 2010. After reviewing and analyzing responses from the industry, the SDT determined it was infeasible to address all of the concerns and achieve industry consensus on CIP-010 and CIP-011 by the planned target date of December 2010. Consequently, the SDT limited the scope of requirements in this posting of CIP-002 through CIP-009 as an interim step to address the more immediate concerns raised in FERC Order 706, paragraph 236. The approach to address the remaining FERC Order 706 directives continues to be developed.

The SDT believes the NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the "bright-line" criteria contained in *Attachment 1 – Critical Asset Criteria* of the draft CIP-002-4 standard.

The draft CIP-002-4 standard and requirements provide a foundation for effective cyber security to protect the systems that support a reliable Bulk Electrical System (BES). After months of deliberation and industry input, the SDT is continuing to evolve the Reliability Standards addressing cyber security by presenting a draft standard *CIP 002-4 – Cyber Security – Critical Cyber Asset Identification* that identifies BES Cyber Systems according to "bright-line" criteria associated with the impact on reliable operation of the BES. The *CIP-002-4 Cyber Security - Critical Asset Identification - Rationale and Implementation Reference Document* provides clarifying notes and rationale of the SDT. The draft CIP-003-4 through CIP-009-4 standards include conforming changes to match the versioning of CIP-002-4.

A separate ballot is being conducted on CIP-005-4, and if the proposed standard is approved it will be filed with CIP-003-4 to CIP-009-4. If the proposed CIP-005-4 is rejected, then the present CIP-005-3 will be modified with conforming changes and filed with CIP-003-4 to CIP-009-4. The team is continuing to work on subsequent cyber security standards that will establish impact levels and define associated cyber security controls at levels appropriate to their BES impact.

The Team is seeking industry feedback and suggestions on this draft of CIP 002-4. The industry feedback will be considered by the SDT in revising and refining CIP 002-4 requirements and related documents.

The SDT has provided a form for industry participants to offer their comments on this draft of CIP-002-4.

Questions

Your responses to the following questions will assist the SDT for Project 2008-06 Cyber Security Order 706 in finalizing the work for CIP-002-4 through CIP-009-4 relative to the proposed modifications summarized above. For each question, please indicate whether or not you agree with the modification being proposed. If you disagree with the proposed modification, please explain why you disagree and provide as much detail as possible regarding your disagreement including any suggestions for altering the proposed modification that would eliminate or minimize your disagreement. The SDT would appreciate responses to as many of these questions as you are willing to supply.

1. CIP-002-4 Attachment 1 contains criteria that define elements that must be classified as Critical Assets. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
2. Requirement R1 of draft CIP-002-4 states, "Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
3. Requirement R2 of draft CIP-002-4 states, "Using the list of Critical Assets developed pursuant to Requirement R1, each Responsible Entity shall develop a list of associated Critical Cyber Assets performing a function essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. Each Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics". The requirement then lists characteristics using the same text that is contained in the existing CIP-002-3 R3. Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

   ☐ Yes
   ☐ No
   Comments:
4. Do you agree with the proposed Violation Risk Factors? If not, please provide suggested improvements on the proposed VRFs.

   ☐ Yes
   ☐ No
   Comments:

5. Do you agree with the proposed Violation Severity Levels? If not, please provide suggested improvements on the proposed VSLs.

☐ Yes
☐ No
Comments:

6. Do you agree with the proposed implementation plan? If so, please explain and provide specific suggestions for improvement.

☐ Yes
☐ No
Comments:

Appendix # 8 Framework Team September 2 Meeting Results

Structure and Composition of CIP Version 5

1) In order to be responsive to: 1) the industry in general; 2) a large industry voting block with far-reaching established programs; and, 3) FERC 706; we need to:

   a) Maintain a size-based paradigm for organizing grid assets. As such, we would define "Classes" of grid assets:
      i) Class A – large ("bright line" CIP-002-4; sans control/data centers)
      ii) Class B - medium sized assets (scope TBD)
      iii) Class C - small sized assets (scope TBD)
      iv) Class D – Control/ Data Centers

   b) Use the NIST paradigm for building requirement-sets; i.e., first establish minimum baseline requirements for all Asset Classes and Categories (see #2 below) for each subject area contained in the CIPs; then augment as criticality increases (i.e., for Class B Categories and Class A Categories)

2) To obtain granularity in requirements desired, establish "Asset Categories" within each Asset Class, and write Requirements appropriate for each:

   a) Generation Category – within each Class A, B, and C
   b) Transmission Category – within each Class A, B, and C
   c) Control/Data Center Category – within each Class A, B, and C
   d) Others?

   [Note movement of control/data centers out of CIP-002 for treatment as a Category]

Drafting Work Process

1) Initially, create separate sub-teams (STs) to work individually on the controls and technical issues that we need to address. Let's not address the governance issues at first, but hold them until we have the framework better defined. [If additional Standards are determined to be necessary, create additional STs.]

2) Define "*What are we defending against*?" As the first step in the process, each ST will research and specify generic known vulnerabilities that CIP Standards' requirements are aimed to mitigate. This is needed to provide foundational rationale for a more granular approach to Requirements-writing, with the aim of avoiding the pitfalls of a "one size fits all" approach under which we currently operate. This approach should reduce both the number of TFE and variability in interpretation.

3) With an eye toward the issues its working on, each ST conducts a review and captures:
   a) specific instructions contained in the CS_706 SAR
   b) specific FERC 706 directives, ensuring coverage of "Post V4" topics

4) Using the list of vulnerabilities from Item #2 work just above, and directives culled from work under Item #3 just above, each ST will begin crafting baseline Requirements for each Asset Category within each Asset Class, using the following resources:
   a) Draft CIP-011 language, regardless of prior organization of material
   b) DHS Catalog
   c) NIST SP800-53 and SP800-82
   d) ??? NISTIR V2 SG Cyber Security WG
   e) ??? ISA99

5) Using the same resources as in Item #4 just above, each ST would then augment the "Baseline Requirements" created under Item #4 just above, with more "Advanced Control and Countermeasure Requirements" as appropriate for each Asset Category beneath Asset Class B, and Asset Class A respectively.

6) As each ST creates Requirements, it must take note of the potential need for coordination/rationalization of language in the Standard it is working on with other Standards being worked by other ST. [CIP could remain "nested" to a certain degree]

7) After 'rationalization' of language across Standards, either task a new ST or have the entire SDT take up the umbrella governance issues.

II/III Outstanding items needing further consideration

1) Data Communications – Do we:
   a. Create a new Standard?
   b. Treat it as a Category of Asset beneath each Asset Class?
   c. Just enhance the existing approach?
2) Can "Baseline Requirements" be:
   a. Strictly "organizational controls" (largely processes and procedures)? Or,
   b. Also additionally technical countermeasures (equipment, SW, etc.)
3) Shall we have different "Baseline Requirements":
   a. Across each Asset Class? [Class A more rigorous than B, and B more than C]
   b. Across each Category within each Class? [Same logic as 3a.]
4) Other areas the Framework Team members want to discuss at this time?

How much farther than this do we want to go before gaining full SDT agreement in principle that this approach is acceptable?

Appendix #9 Sub-Team Roster

Sub-Team	
CIP 010 BES System Categorization	John Lim (Lead), Rich Kinas, Jim Brenton, Dave Norton *(Observer Participants: Rod Hardiman, Jim Fletcher) (FERC: Mike Keane, Peter Kuebeck)*
Personnel and Physical Security	Doug Johnson (Lead), Rob Antonishen, Patrick Leon, Kevin Sherlin *(FERC: Drew Kittey)*
System Security and Boundary Protection	Jay Cribb (Lead), Jackie Collett, John Varnell, John Van Boxtel, Philip Huff *(Observer Participant: Brian Newell) (FERC: Justin Kelly)*
Incident Response and Recovery	Scott Rosenberger (Lead), Joe Doetzl, Tom Stevenson (*Observer Participant: Jason Marshall) (FERC: Dan Bogle)*
Access Control	Sharon Edwards (Lead), Jeff Hoffman, Jerry Freese, Bill Winters *(Observer Participants: Roger Fradenburgh, Robert Preston Lloyd) (FERC: Mike Keane)*
Change Management, System Lifecycle, Information Protection, Maintenance, and Governance	Dave Revill (Lead), Jon Stanford, Keith Stouffer, Bill Winters *(Observer Participant: Brian Newell) (FERC: Jan Bargen, Matthew Dale)*
CIP 002-4 Drafting Team	John Lim (Lead), Jim Brenton, Jackie Collett, Jay Cribb, Sharon Edwards, Doug Johnson, Rich Kinas, Dave Norton, Dave Revill, and Bill Winters *(Observer Participants: Rod Hardiman; Jim Fletcher; Bryn Wilson) (FERC: Mike Keane, Peter Kuebeck; NERC: Scott Mix)*
Implementation Plan CIP 002-4	Dave Revill (Lead), Sharon Edwards, Kevin Sherlin, Scott Rosenberg, Dave Norton and Phil Huff *(FERC: Mike Keane; NERC: Scott Mix)*
Framework CIP 010 &011	Dave Norton (Lead), Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. *(FERC: Mike Keane; NERC: Scott Mix)*