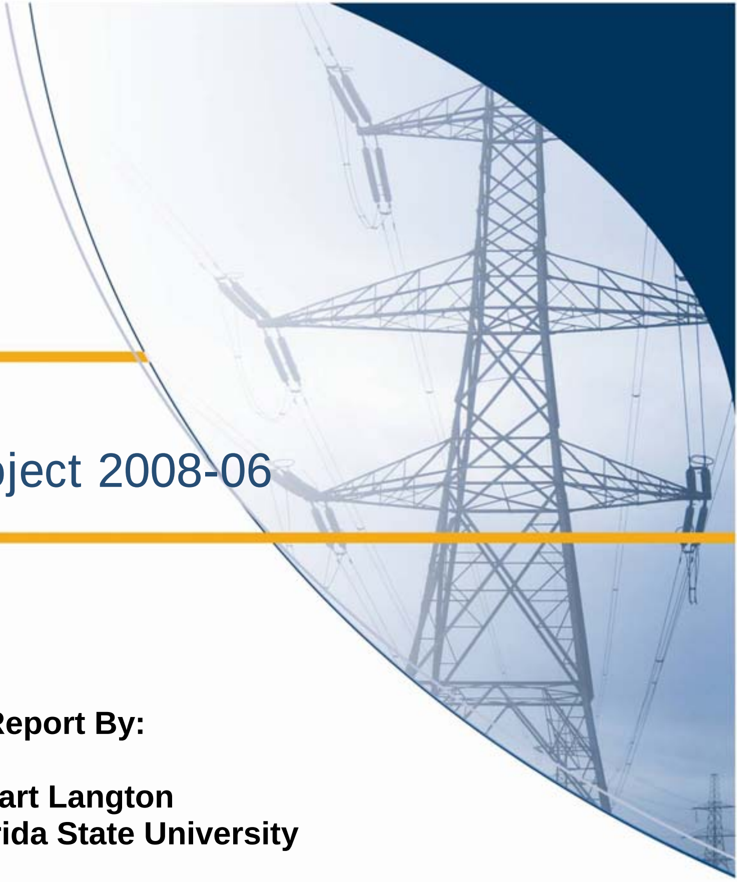
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION



Draft Meeting Summary

Cyber Security Order 706 SDT — Project 2008-06

December 4, 2008 | 8 a.m.–5 p.m.
December 5, 2008 | 8 a.m.–5 p.m.

SDT Draft Meeting Report By:

Robert Jones and Stuart Langton
FCRC Consensus Center, Florida State University

Thanks to Team members Sharon Edwards, Tom Hofstedler and Kevin Perry for sharing their meeting notes.

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

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

Cyber Security Order 706 Standard Drafting Team
Draft December 4–5 Meeting Summary
Washington D.C.

Meeting Summary Contents

Cyber Security Order 706 Standard Drafting Team
Draft December 4–5 Meeting Summary
Washington D.C.

EXECUTIVE SUMMARY

The Chair, and Vice Chair welcomed the members and a roll call of members and participants in the room and on the conference call was conducted. Following review of the proposed meeting agenda, Michael J. Assante, NERC Chief Security Officer who offered some comments and perspectives for the Team's consideration urging them to adopt an "outcome oriented" standards development approach with a goal of regulatory stability while focusing resources on protecting what is most important. Jake Olcott, Staff Director and Counsel, House Subcommittee on Emerging Threats, Cyber Security, Science & Technology chaired by Rep. James R. Langevin (D-RI) under the Committee on Homeland Security, offered comments on the Team's effort thus far and noted that this was an area to great and continuing interest to Congress, as witnessed by their formal comments submitted by the Committee and Subcommittee on the FERC Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection in October, 2007.

David Taylor reviewed with the Team the need to comply with NERC's Antitrust Guidelines.
The SDT unanimously adopted the November 12-14, 2008 meeting summary with a correction in the text changing the quorum rule from 51% to 2/3's. The facilitators reviewed with the Team the consensus guidelines adopted at the Little Rock meeting.

Kelly Ziegler, NERC Manager of Communication presented a proposed Phase I Communications Plan. She outlined for the team three plan objectives: provide adequate information for voting**;** improve visibility of the SDT process**;** and drive positive media coverage**.** She then described the Webinar procedure and NERC's experience with them.

Scott Mix reviewed the "Technical Feasibility eight page document which was first reviewed at the Sacramento meeting and then again at the Little Rock meeting. The paper sections include:

- Objective/Purpose/Executive Summary/Background
- Definition of Technical Feasibility Exception:
- Application:
- Overview of Essential Elements:
- Detailed TFE Process:
- Good Faith efforts
- Sensitive Information:
- Post Approval Processes required by FERC Order:
- Appeals Process:

This was modeled after self-reporting mechanism to fit into the existing compliance program. He noted the plan was to post a white paper for Industry review after the Team reviewed and agreed on the draft. Todd Thompson, NERC Compliance, noted a process has been developed for protecting sensitive audit-related information so it remains on site at the Responsible Entity, providing evidence if it's tampered with. Roger Lampila noted that training is being provided to regions for their CIP auditors; during recent session, there was general agreement from those present that more knowledgeable auditors will be needed. Entities need to verify with their respective regions that the individuals performing the audits are qualified.

Areas of the Paper the SDT commented on included: Documenting Mitigation; Remediation Steps and Wide Area Approval- ERO's audit process--Regional Entity and ERO Steps

Scott Mix sent out the TF Exception Paper for review by the drafting team on Thursday evening. Comments were received from several drafting team members and Mr. Mix responded on Friday with refinements to the draft. Mr. Mix agreed to determine how the paper would be presented to the industry- i.e. as a NERC or SDT product. The Team agreed to provide Scott with comments by December 12, 2008 and the SDT would review the revised white paper at the January meeting seeking to adopt it for posting thereafter for industry comments.

The balance of the meeting focused on reviewing and discussing the approach to the SDT's Phase II which had been reviewed at each of its first three SDT meetings including an options paper presented and discussed at the Little Rock meeting.

A presentation on the implementation of the NIST framework from a user's perspective was offered by SDT members Jeri Brewer, John Stamford and Keith Stouffer. They provided some perspectives on implementation and identified issues. Following the briefing, The SDT members discussed current approaches to identification of Critical Assets, risk management and the following topics:

- New Technology and Risk Management
- Threats and Risk
- NIST Guidelines and CIP Standards- Both/And?
- Risk Assessment and Resource Implications
- Component-based System Approach
- IT and Control Systems
- Levels of Risk- “One Size Fits All”? NIST and CIP
- Compliance and Audit Concerns

Following the Little Rock meeting, the facilitators asked the Vice Chair, Kevin Perry to draft some strawman draft statements and questions to serve as a starting point for the SDT's consideration of risk assessment. He introduced the statements noting they provide a statement on the industry's current methodology, a problem statement on this methodology, and 8 critical questions regarding risk management. The SDT reviewed and discussed risk management and tested the support through a 4-point acceptability ranking for the following statements:

The Current “Consequence-based” Assessment Methodology Draft Statement:
The industry focuses on the facility (asset), employing a “consequences-based” assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:

- Those that are essential are declared to be Critical Assets.

- We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

(Average Acceptability Ranking-3.9 of 4)

A Draft Problem Statement with the "Consequences-Based" Assessment Methodology:
The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa. *(Average Acceptability Ranking-3.8 of 4)*

(b) The industry may be "cherry-picking" the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment. *(Average Acceptability Ranking-3.1 of 4)*

- *2nd Draft* (b) Some in the industry may be selecting the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment based on economic vs. security considerations.

(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector. *(Average Acceptability Ranking-3.1 of 4)*

(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System. *(Average Acceptability Ranking-3.8 of 4)*

The discussion regarding risk management led to the testing of the goal of CIP 002. The following statement was offered for acceptability ranking:

> The goal/intended outcome of CIP 002 to identify the Cyber Assets (i.e. Programmable electronic devices and communication networks including hardware, software, and data, NERC Glossary) that need to be protected and to identify the level of protection. *(Average Acceptability Ranking-3.8 of 4)*

The SDT then discussed what kind of framework made sense for inventorying cyber assets which covering the following topics:

- Overall Approach
- Inside-Out Approach
- Systems View
- Protection Model
- Scope
- What Assets Included?
- Real World Examples
- Inventory and Compliance

Following the discussion, one member proposed testing support for the following inventory statement:

Inventory your cyber assets directly related to the operation of your registered NERC functionality:

- Apply a risk methodology to assign a level.
- Apply distinct controls according to the level.
- Inventory for each cyber asset should be: device + o's + function + firmware level.
- These attachments will be critical for patch management and CIP 007R1 testing.

(Average Acceptability Ranking-2.3 of 4)

Another member then proposed testing support for the following inventory statement:

> Identify the applications and computer systems within the Industry Controls Systems or information systems as well as the networks within and interfacing with the ICS. The focus should be on systems rather than devices, and should include PLCs, DCS, SCADA, and instrument bases systems that use a monitoring device such as an HMI.
> *(Average Acceptability Ranking-2.2 of 4)*

Following the lunch break on Day 2, the chair announced that Jackie Collett and William Winters had agreed to draft two “straw” documents, reviewing the SDT discussions to date, to help move the Team forward on the development of a Phase 2 roadmap:

- SDT member Jackie Collett will draft a white paper starting from an attempt to protect the best of what exists with the current CIP and incorporating NIST concepts/features.
- SDT member William Winters will draft a 2nd white paper starting with the NIST framework and incorporate the best of the CIP into it.

NERC staff presented some information and sought SDT input on the industry “Webinar” December 16 from 11:30 until 1 p.m. on the Phase I SDT products. The SDT reviewed the proposed meeting schedule to complete the Phase I process by the end of June, 2009. The next meeting will take place at the Arizona Public Services Corporation facilities in Phoenix. The Chair suggested the following agenda items:

- Organizing and initiating the review of industry comments that have been received on the posting of Revised CIP standards from Phase I;
- Finalize the SDT input to the NERC Technical Feasibility Exceptions white paper; and
- Time permitting, continue discussion of the CIP 002 approach to assets in scope for Phase II including review of the papers from SDT members Jackie Collett and William Winters.

At the conclusion of the meeting, the facilitators asked the Team to offer an evaluation of the process including what worked well during the meeting and what could be improved. There was appreciation of the meeting site in the Capital and facility, of the sound system, of the tagging on from the NERC CIPC meeting and the debate and breadth of knowledge on the team. On improvements, SDT members suggested the facilitators should try to close off open-ended discussions where we are repeating our points (i.e. “violent agreement”). The meeting adjourned at 2:15 p.m. Friday afternoon.

Draft Fourth Meeting Summary
December 4–5, 2008
Washington D. C.

I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair, and Vice Chair welcomed the members and asked NERC staff David Taylor to conduct a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the Team and participants the proposed meeting agenda *(See appendix #1*).

The Chair introduced Michael J. Assante, NERC Chief Security Officer who offered some comments and perspectives for the Team's consideration. He thanked the Team for their commitment and work to date and urged them to adopt an "outcome oriented" standards development approach which will require rigor and discipline to follow through. He suggested the key goal should be regulatory stability – i.e. seek to establish an enduring outcome with a set of standards that will last for long time – only needing tweaking as conditions change. This will require a very sharp focus by the Team on each requirement to define the outcome you are trying to achieve and then work backwards to ensure all of the requirements achieve the desired outcome objective. To illustrate the offered two examples:

- CIP-002: approach understood, objective well intended, trying to take sensible approach to defend what is most important. But if you do work backwards, you will find gaps that need to be filled. Guard against assumptions that if you do it right you will fill the gaps. How dangerous are the assumptions? TO/TOP understands assets and can make determination of relative importance. Not true of GO/GOP that do not have planning resources.
- CIP-004: Personnel Risk Assessment/Training – plan is good, subject matter of training will change. If outcome is to assure that risky personnel cannot have unescorted access to cyber assets, then working backwards you find gaps. A missing gap is an entity must have a list of disqualifying factors. A starting point may be the Federal standards (Transportation Worked Identification Credential) a federal mandate for any entity needing access to port facilities. Then need to bring in bargaining agreements, etc.

The Team should focus resources on protecting what is most important. The CIP standards requirements may not have that focus and there may be some gaps. He challenged the Team to look at each assumption with this in mind and suggested their Phase 2 work is the right time to deliver this message.

The Chair also welcomed Jake Olcott, Staff Director and Counsel, House Subcommittee on Emerging Threats, Cyber security, Science & Technology chaired by Rep. James R. Langevin (D-RI) under the Committee on Homeland Security, and invited him to provide the Team with any comments. Mr. Olcott acknowledged the Team's effort thus far and noted that this was an area to great interest to Congress as witnessed by their formal comments submitted by the Committee and Subcommittee on the FERC Notice of Proposed Rulemaking for Mandatory Reliability Standards for Critical Infrastructure Protection in October, 2007 *(See Appendix #9).* He noted that membership is not yet resolved for the new congress but predicted that there will be continuing interest in this topic. He noted that the Energy and Commerce Committee in the House and Senate are also very interested in this issue. He noted that he will be following the Team's work and provided his contact information for anyone wanting to follow up with him *(See, Appendix #9).*

David Taylor reviewed with the Team the need to comply with NERC's Antitrust Guidelines *(See, Appendix #3).* He urged the Team and other participants in the process to carefully review the guidelines as they would cover all participants and observers. He urged all to avoid behaviors or appearance that would be anti-competitive nature and also reminded the group of the sensitive nature of the information under discussion.

The Chair noted the November 12-14, 2008 meeting summary had been circulated to members in advance of the meeting. She noted a correction in the text changing the quorum rule from 51% to 2/3's. David Norton moved and Sharon Edwards seconded the motion to accept the summary as revised. The Team unanimously accepted the meeting summary.

The facilitators reviewed with the Team the consensus guidelines (Appendix #5) adopted at the Little Rock meeting.

II. NERC PHASE 1 COMMUNICATIONS PLAN

Kelly Ziegler, NERC Manager of Communication presented a proposed Phase I Communications Plan. She outlined for the team three plan objectives: provide adequate information for voting**;** improve visibility of the SDT process**;** driving positive media coverage**.** She then described the Webinar procedure and NERC's experience with them. They will provide a press release in advance which will note the multi-phased approach and a high level summary on the web of the Phase 1 products.

Initial Questions/Comments on the Communication Plan Approach

- Reference to 3 phases? Should be referenced as a multi-phase approach.
- It would be ideal to capture the audio webinar in a-podcast form so industry could listen to it at other times.
- Press release: timing? Plan to released next week followed up with the Webinar.

III. TECHNICAL FEASIBILITY EXCEPTION- REVIEW AND REFINEMENT

Scott Mix reviewed the "Technical Feasibility eight page document which was initially reviewed at the Sacramento meeting and then again at the Little Rock meeting. The paper sections include:

- Objective/Purpose/Executive Summary/Background
- Definition of Technical Feasibility Exception:

- Application:
- Overview of Essential Elements:
- Detailed TFE Process:
- Good Faith efforts
- Sensitive Information:
- Post Approval Processes required by FERC Order:
- Appeals Process:

This approach was modeled after self-reporting mechanism to fit into the existing compliance program. He noted that he would go through a red line version for one more round. He reviewed the requirements within the filing including the date that the TF exception is no longer necessary. After the individual filings are made, FERC has charged the ERO with the task of taking a regional and national impact of all TF exceptions. At this time, NERC does not have a consistent process for self-reporting across the regions. The TFE language may show up in 005 & 006 & 007. There were many questions concerning the right approach to presenting the straw man to the industry.
He noted the goal would be to post a paper approved by the Team for comment soon after the December or January meeting.

Todd Thompson, NERC Compliance, noted a process has been developed for protecting sensitive audit-related information so it remains on site at the Responsible Entity, providing evidence if it's tampered with. Roger Lampila noted that training is being provided to regions for their CIP auditors; during recent session, there was general agreement from those present that more knowledgeable auditors will be needed. Entities need to verify with their respective regions that the individuals performing the audits are qualified.

SDT Comments

- If we do our job right we will look at outcome-based standards. The issue is that the standard does not drive technology and that the proposed process needs to consider requirements that apply to PLCs, for example, where there is no solution in response to the requirement such as anti virus.
- Order 706 may leave room to consider replacing equipment that does not comply with the requirements with a similar vintage of equipment if necessary.
- NERC might start an effort to work with the vendors to supply solutions to security as directed in Order 706. This would be something that the ERO could do to improve and drive technology.
- Where ever possible take care of this in Phase 2. But will need a process to deal with really new problems.
- Could be a self-reported non-compliance?
- Some technical requirements may mean someone may need a TFE. Indicate in general language a requirement that you think the TFEs showing up will be reviewed on a case-by-case basis analysis.

- What about an instance of, for example, a plane crash with all staff? Self report of non-compliance. Not a technical issue but an emergency issue.
- You may need an "exception" to the exception process- "outcome basis"? Let the ERO deal with it. If denied then on the non-compliance path. If accept, look back at whether standards need adjustment.
- Each utility for each requirement, e.g. CIP 007- file an exception per requirement, per utility? Could be a deluge? Checks and balances will require paperwork associated with it. Consider the compliance process- self reported
- This may be the reason to stop thinking about generation, transmission and think about types of equipment. All bought at same time, with same problem. E.g. 10,000 of a brand of relays that can't support a password. Single filing vs. 10,000 filings. Will have to work through details
- TFE- problem with piece of equipment- probably would result in one filing.
- The required timeframe for documentation may present problems.
- Consider a paperwork avoidance procedure—while we annotate where TFEs can be taken.
- Develop a list where we know where exceptions <u>can't</u> be taken. When does the inconvenience/cost factor cross over into a security issue. "Infeasibility"- can't be just inconvenience.
- "Burning the strawman" in the debate- put this in a guideline. Cut down on lots of needless actions.
- Clarification- TFE procedure – same as CIP 003 R3 exception process? No. Difference. R3 is taking exception to own internal policies and not a compliance issue vs. a compliance issue taking exception to the standard.
- If built policy to mirror CIP standards, would they be interpreted as one and the same? You may do that but the ERO won't be tracking all internal policies at a company.
- If we do our job right and focus on outcome based standards this will be addressed.
- Today no consideration in current standards as to whether their application makes sense in a particular setting. Concept deserves continued debate and discussion.
- Standards do not drive technology- can't expect that sometime in future engineers will design a way to comply with standard. Also can't assume technology won't change.
- Opportunity for NERC to document the current exceptions taken to date to inform the SDT review of this? Probably right thing to do. List sounds like a roadmap to the past. How to communicate all info to all who need to take action and yet protect everyone else. Difficult problem. Devil in the details.
- Operating systems- software and purpose written software do not have the same vulnerability.
- "Improperly comply with requirement"? Literal interpretation reducing reliability. E.g. passwords not working well in a setting.
- Maybe this is literally complying vs. "improperly"
- Revision in Phase 2 should be more obvious where to apply
- Virus scanning- putting on windows platform becomes a detriment to the operation.

- Clear as to what we are asking for. E.g. list what not complying with and provide mitigation steps. Need to understand- dealing with the remaining risk or risk of not doing it at all.
- Can’t anticipate everything. Probably can be clear on somewhere you can’t take a TFEs.

Documenting Mitigation- *Scott Fix, NERC*

- Documenting mitigation. E.g. protect device from attack from viruses by doing something that isn’t in the standard but works.
- Document a remediation plan- will be long term plans. May be open-ended plans. “when it breaks I will fix it”. Need provision for these kind of plans. Tough to do with annual approval process.

Remediation Steps

SDT Comments on Remediation Steps

- Envision a technical exception to equipment password. Still purchasing equipment. So taking a TFE of where they are going, not just where they been.
- E.g. 100,000 relays in environment. 1 breaks do I replace with one everyone knows how to work with or the new one requiring new training, assessment, major purchases. Different from a new substation investment. Everything should meet standards.
- Everything done is very date-related in terms of compliance looking backwards.
- 706 position may not be right on remediation by date certain necessary in all cases.
- Para 181- new equipment- left some wiggle room for valid considerations
- NERC compiling exceptions? Can’t write standards that drive the vendor community? Need to ask for a bridge that is not too far.
- What NERC might do, start working with vendors in a vendor management forum to educate and help the market respond better. Feed into this concepts like forensics?

Wide Area Approval — ERO’s audit process — Regional Entity and ERO Steps

SDT Comments

- Front line for the process. Notice to the Region on TFE.
- Region apply catalogue i.d. to track- analysis and approval
- ERO needs to provide enough info for Regional entity to do job
- If not enough detail provided, claim rejected.
- Analysis of impact to reliability of TFE. Might require coordination with other entities and regions.
- Milestone slippage- grounds for non-compliance. In best interest to be upfront and forth coming.
- Sensitive info concerns. E.g. Fed agencies for FOIA requests etc.
- Post approval process- annual report to FERC. Canadians have a similar view in their systems. ERO high level view across America. “ARSAWS” (check with todd) completed for all requirements.

- Didn't invent a new appeals process. Compliance and enforcement monitoring appeals process.
- Safe harbor/good faith while request is being processed? CMEP is public document. Is this legal? FERC safe harbor wasn't thrilled. May open up self to "gaming"- have to structure it carefully.
- Cryptographic mechanisms? E.g. Disaster recovery evidence go with it. Including this for electronic documentation. Incorporated way to take encrypted data on better cds. Maintain it at responsible entity.
- Summary info to Canadian entities. Responsible entity has some sort approval? Utilities need some input on what goes forward. Regional entity, ERO and utility should be comfortable. Work towards getting something that meets all needs before reporting.
- If you go to ERO and they say no to TFE? Use the appeals process at the ERO.
- Has to be added to each regional entities CMEP for this to work. This is part of the next steps. Sooner we do this, better we will all be.
- Guidance from current compliance self report process?
- Better definition of "validity"? Fair question. Need to clarify that for industry.
- Part will be how well you write justification and how you demonstrate that you are seeking to achieve the spirit of the requirement.
- Do the RE's have the technical expertise to evaluation the appropriateness of the TFE? Typically don't know various systems. How will we expect that can do this consistently across.
- Reason why approvals are multi-step. ERO could reject even when the RE accepts.
- May become part of the formal delegation agreement?
- How good is good enough? Adequacy metrics. Regional auditors- ARSAW run through to see how vanilla IT look at cyber security environment.
- FISMA experience- Keith. SP 800 series is a lot of guidelines- best professional advice.
- SDT can't do this. Is there an encyclopedia can go to in order to help with the process.
- Federal agency- Auditor General- take a manual- (Jeri). Reports to congress annually on how effective Federal agency security program. Effectiveness of your implementation against the 853 standards. How well that is achieving the goal. FISCAM- Audit Manual
- 800 series documents have lots of best practices. Most are guidelines. GAO looks at them, says you can't blow off, must consider. Some weight.
- Unfortunately for this area are IT specific vs. cyber. 800-82 is one guidance doc. ISA 99 good material as well.
- Don't overplay how "unique" our environment increasingly is.
- Field assets are a different animal.
- This is bigger than just TF, also auditing requirements of regions. Problem recognized within the compliance structure- regions told need to solve the problem. ERO is serious as well with Mike and Todd brought on.
- First CIP auditor training recently in Princeton. Just getting underway. By the end of day 1, regions realized they needed more talented staff. Only a few with the right background. Really thinking of how to function as a audit team member.
- NERC- virtual auditor- support structure to get assistance and reach back.

- What assurances do we have this will be done before audits are happening? Auditing bodies should show how their training. This is a major concern of industry. This is a resource and knowledge issue.
- Federal- auditing with key focuses- programmatically how applied the standards and guidance. Did we id the risks and select the right controls. Test the controls to determine level of veracity and then produce a report (GAO, IG) give equal weight to IT and the cyber community. Have to do risk assessment.

Next steps — Day One

- Scott Mix will clean up and email to the team.
- SDT members will provide comments and suggestions.
- NERC internal working document and doesn't have to go through a ballot process.

SDT Comments

- Are we sure the requirements won't change. TFE for other than technical issues. Invoked where it allows. How to handle this? Hold off until we hit the version 3 standards.
- "Field test" the process.
- If this guideline is to be treated as a non binding guideline then no voting necessary. If this is the expectation that auditors will use and will become binding, industry will have to vote on it.
- This document needs to fit into and follow the current ERO auditing process.
- NERC – Roger's process for input on the audit process. Went to NERC BOT for approval. CIPSE guidelines don't go to BOT because they are not binding. Some way these will be sanctioned.
- Need to make this when implemented. Need to say where this TFE cannot be used.
- FERC- identify where positively can't be used. "Willing to be reasonable" TFE process will be out quickly and implemented quickly.
- Note, when we revisit the requirements- its only where it is currently in the standard.
- Possible at beginning of Jan meeting to agree to post.
- Do we apply only where we have it in the standards?
- Back out "only where specifically allowed" language. Note we may do this in Phase 2.
- Deleted "reasonable business judgment and acceptance of risk"
- Team appreciated.

Day Two — SDT Review and Next Steps

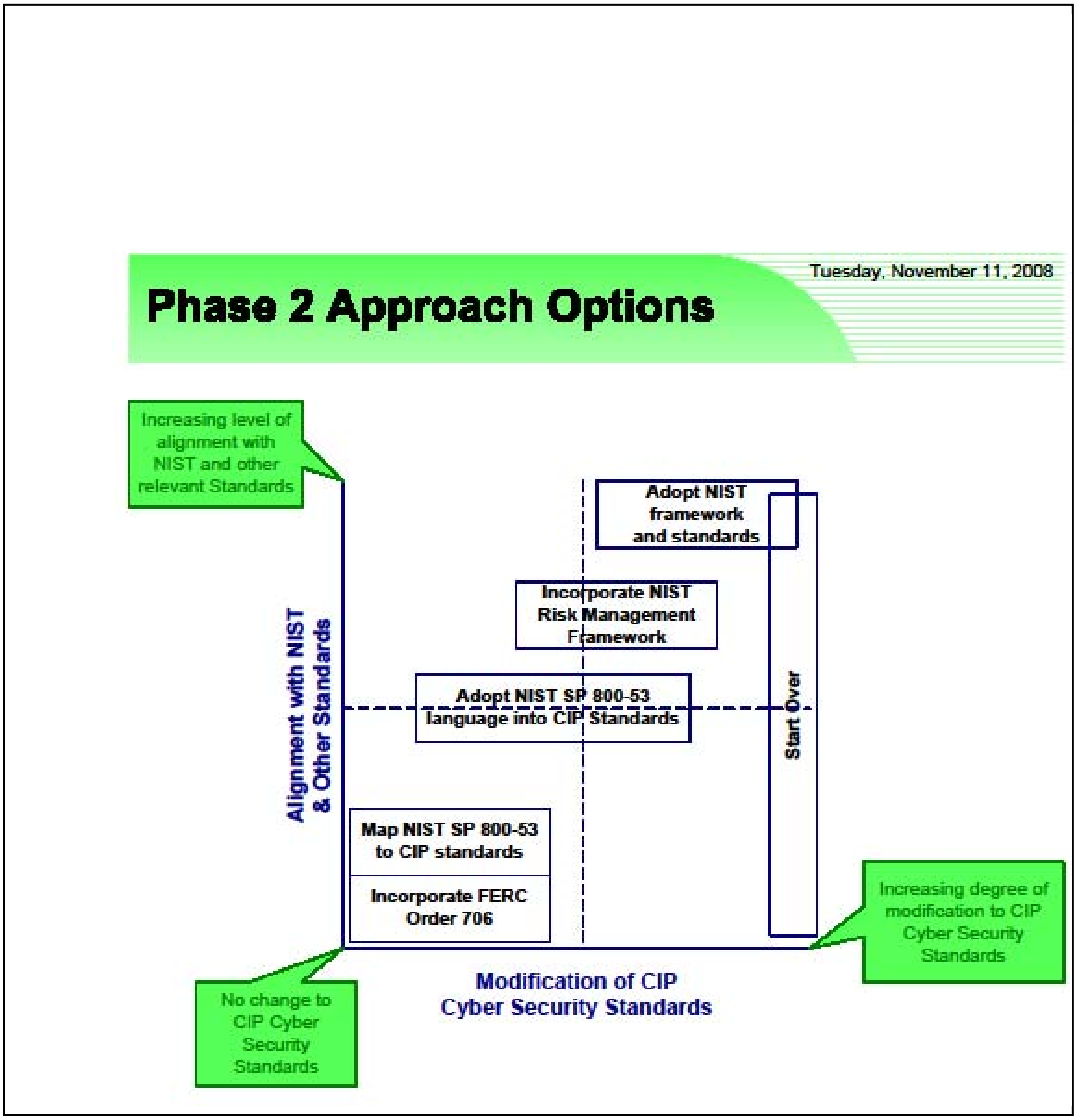
- Scott Mix had sent out the TF Exception Process for review and sent it out to the drafting team on Thursday evening. Comments were received from several drafting team members.
- There was a concern expressed around sensitive information. Scott stated that NERC staff will review the procedure with audit staff. Scott said he would like a couple more days for the rest of the drafting team to review and make comments. After that the draft will be sent out to the drafting team PLUS list.

- Scott also wants the legal staff to review. After all those steps are done, the information will be posted as a white paper for public comment.
- Scott does not expect the public posting to happen until 1st half of January. Scott raised the issue of whose name should be on the white paper when it is posted?
- When the team provides comment, Scott asked that the group provide questions that should be asked of the industry at the public posting.
- The Chairman suggested Friday, December 12, as the due date for comments. The Facilitator asked that comments be submitted to the entire drafting team.
- The technical feasibility exception is in the standard today. What NERC is creating is the procedure that utilities must follow so the change that is being proposed is a change in the rules of procedure. Therefore, this is not a new standard; the TF exception is a new NERC process. There was discussion as to whether NERC needs to post the document for public review. It was generally agreed that the new TF exception process is only a NERC procedure not a standard, and does not need to be balloted by the industry.
- This process provides approval, oversight and appeal. Order 705 Paragraph 184 - exemption is a release from a requirement; an exception is a way to deal with a requirement. There was discussion of the meaning of "exception" vs. "exemption."
- Jeri cautioned the group to get their comments in on the TF exception process. Finalizing the SDT review of the Technical Feasibility Exceptions white paper will be placed on the SDT agenda at the January meeting.

IV. REVIEW OF PHASE II APPROACH

A. Background on SDT Development of Phase II Roadmap

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



Phase 2 Approach Options

Tuesday, November 11, 2008

Increasing level of alignment with NIST and other relevant Standards

Adopt NIST framework and standards

Incorporate NIST Risk Management Framework

Adopt NIST SP 800-53 language into CIP Standards

Map NIST SP 800-53 to CIP standards

Incorporate FERC Order 706

Start Over

Alignment with NIST & Other Standards

Increasing degree of modification to CIP Cyber Security Standards

No change to CIP Cyber Security Standards

Modification of CIP Cyber Security Standards

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

B. Perspectives on Implementing the NIST in the Context of the CIP

SDT members Jeri Brewer, John Stamford and Keith Stouffer provided some comments on implementing the NIST framework from a user's perspective

1. Briefing Issues Identified

- NIST was established around human relations and finance style systems. It was not based on the operational perspective of a control system that needs to keep the operations functional 24/7 minimizing disruptions when they happen (nature, troublemakers etc.). The NIST risk management framework gives tools from IT to apply to control sectors that give protections. 882 helped to address some of the gaps between the IT and control system perspectives.
- The basic concept calls for identifying assets and the risk these assets will have on your mission and tailoring the protections to fit your mission needs.
- Focus on is on control systems, so production impact is a greater concern than in IT. NIST Framework is tool designed for IT environment and applied to control system environment. Elements missing from 800-53 have been addressed by 800-82.
- So NIST represents a process for identifying assets and the associated risks, with protection tailored to fit systems and environment is based on impact, what is needed to address it.
- The NIST framework provides a way for the utilities to adopt the methodology tailored to the utility's specific needs.
- On the positive side, the NIST framework is technology neutral. It is “technology agnostic and risk agnostic.”
- The NIST risk management framework is also flexible for tailoring. However this can also be a negative in that it requires more work and expertise of the end user and in the control center environment to figure out how to align the system. This also extends to the auditor in determining how to assess your system. In a compliance environment the CIP standards tend to lend themselves to more prescriptive requirements--more check-the-box than risk management.
- It functions like an IT network environment with common platforms. NIST framework adapted well to the control system environment. Started in 2004 in first NIST draft.
- The NIST framework has adapted well to the control system environment, however they have not been as successful in adapting the framework for field devices which are not similar to normal IT systems on which NIST was based initially.
- This framework is superior to other methods which are available.
- In a compliance environment, more prescriptive directions for the NIST framework may be needed to facilitate auditing.
- Investing resources to give the biggest bang for you buck. Not 100% protection. Focus on minimize disruption on critical operations, get them back into production as quickly as possibl**e**
- Framework to structure and invest in those resources so you can be resilient and recover quickly.

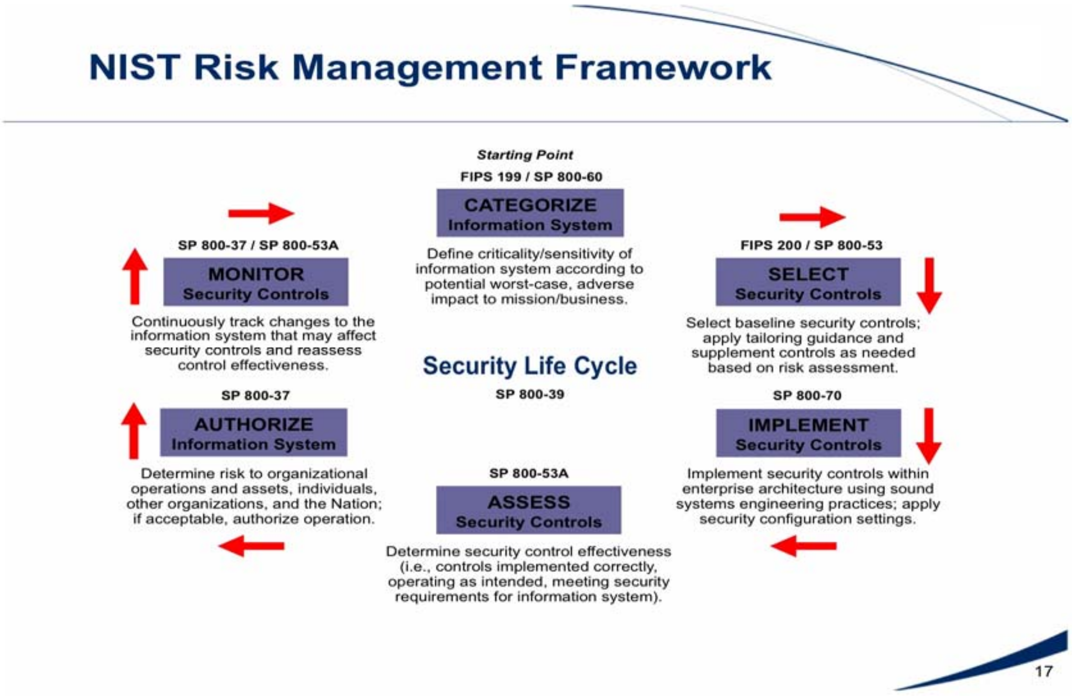
- Standardized way to establish protections with flexibility to adapt to requirements and assets to meet mission.

SDT Comments on NIST and CIP

- The SDT members discussed current approaches to identification of Critical Assets, the role of threats, and associated matters.

2. New Technology and Risk Management

- New risks are constantly being introduced as a result of bringing on new technology. This trend will continue.
- In the field this is a much bigger challenge. Smart grid and substation automation is happening and easier to consider in this light.
- Increasing use of intelligent electronic devices.
- A fundamental issue: mindset in the industry that doesn't take interconnectivity of systems into account.



NIST Risk Management Framework

Starting Point
FIPS 199 / SP 800-60
CATEGORIZE Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

FIPS 200 / SP 800-53
SELECT Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

SP 800-70
IMPLEMENT Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

SP 800-53A
ASSESS Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

SP 800-37
AUTHORIZE Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

SP 800-37 / SP 800-53A
MONITOR Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle
SP 800-39

17

3. Threats and Risk Management

- Congressional perspectives frame the issue in terms of how the model addresses threats and vulnerability. Congressional staff are looking for feedback from the SDT on how that fits into the NIST or other risk management models used by the industry.

- In the federal NIST implementation framework, most threat information comes in from DHS.
- Frankly in the federal sector from a substation control center perspective, Congress needs to sit down with people who do this every day. Homeland security data is largely worthless, as it is very generalized threats. Doesn't apply specifically to the grid and electric system.
- In recent Audit- DOE was criticized for not having good external threat information, even though it is reliant on DHS for this data.
- If you know your vulnerabilities, considering "risk" isn't viable because true risk is impossible to ascertain. Instead, the focus should be on the vulnerability & the impact if it occurs. Whatever has the greatest potential impact is the area that needs the greatest effort to protect.
- FERC suggested that threat should be taken off the table when it comes to a risk assessment. Instead look to take the best of CIP and NIST in order to provide better protection for control systems. Field devices are going to need minimal amount of protection. But there is a basic level of protection regardless.
- Internal threat profiles are frequently overlooked in many risk assessment discussions.
- We should use a consequence-based assessment- what is the consequence of comprising and taking over the system vs. just knocking the system down.
- Threat- many people believe government has good threat information. But it really isn't there or if it is, it is only available for short term (vs. longer term).
- In the risk equation, throw threat out otherwise it drives the risk lower. Never will get the granularity you want.
- For the industry the threat/risk is sanctions. Our vulnerability is unclear. Potential to separate the critical asset assessment from the standard itself.
- What is the vulnerability of BES from any asset we control. Drive down to risk assessment- do we employ a graded-mitigation model? With a high risk, there will be a higher level of mitigation. Not a proponent of low-level mitigation.
- Missing vulnerability information related to our assets. No model in place for determining the effect of the loss of a given asset. E.g. that component has the following vulnerability.
- Have to take the vendor's assessment of that.
- Concern about the quality of the vendor companies for the assessment. National labs available to do this. Get additional funding not just from the industry.
- Develop a national security assessment model?
- Is exclusion of vendors from the standards development a problem?

- Threat and vulnerability- last posted draft of the CIPC- "threat and vulnerabilities" are going to exist. Becomes an impact analysis for the reliability or operability of the BES. Risk based assessment method- does an asset if destroyed impact the reliability of the BES.
- Threat and vulnerability should be irrelevant. Impact analysis is what matters and it is what we do best.

4. NIST Guidelines and CIP Standards — Both/And?

- Is there a key difference between guidelines vs. a standard? CIP is already using a lot of the framework. When the industry re-did the CIP standards, it took a risk-based approach. Sees a lot of good points from NIST that could be added to the CIP standards.
- Most valuable aspect of FISMA framework is doing the risk-based approach to whatever asset you are dealing with.
- While it is not easy to implement, it is superior to others e.g. ISA 99.
- Based on the CIP and NIST experience evidence suggested it may be possible to use both standards and controls to help strengthen the CIP.
- NIST is proscriptive to systems applied to. Hardware, software, people and processes.
- Can do things in field you can't do in CIP. Look at like assets. Mitigate risks to assets in a repeatable way.
- CIP is all or nothing. Black or white. CIP standards are more requirements. Put you in a path you may not be able to get out of.
- NERC assessment- Bonneville is self-funded not subject to appropriations. When NERC a non-compliance finding happens, it is taken very seriously. The SDT job is to marry the two approaches together so we are not wasting time, effort and resources.
- The SDT should use the concepts of the framework and not the specifics—that's what the SDT needs to focus on. Industry needs reasonable and achievable controls, giving them options where appropriate.
- Ideally, adopt the best of CIP & NIST. CIP's biggest problem: identification of critical assets. If protection is focused on those items alone, the other assets related to control systems are left potentially vulnerable. A minimal level of protection would be identified if an organization used NIST process. Everything needs some protection; the most essential assets need more protection.
- The NIST standards & FISMA are not focusing efforts from a national perspective; that's a core problem for this industry to look at issues from this viewpoint.
- This approach is valuable because the oversight responsibilities of NERC & the Regions will offer a different perspective than government utilizes for addressing issues of national concern that extend beyond the boundaries of a specific agency/organization.

Day Two SDT Comments

- Every federal system has to meet baseline controls at a minimum
- Concern that CIP didn't meet even minimum baselines compared to NIST

- Determining scope is an application specific issue; preliminary activities are needed regardless of approach. CIP takes more piecemeal approach and then applies all rules to what's been identified.
- NIST is more systems oriented; looks at identify boundaries around important things, then all aspects of each identified information system are managed—things over which you do have control. A risk based decision needs to be made about what will (or should) come across interfaces from outside that environment. Since every component is not equally able to apply controls, there is a more comprehensive approach.
- NIST may not be readily auditable so it will be a challenge to modify that approach for our purposes.
- CIP vs. NIST. Better adapting the best of each to come up something better.
- Flaw of the "critical asset" — cyber is a different animal can get to all assets at the same time (#274 control stations/centers). N-1 method of id critical assets is not good enough.
- NIST- what is electrically important to the grid- armor those assets. But need to provide basic protection for the rest.
- Resources using the NIST framework are ultimately aligned in most effective manner and threats are not (and cannot be) eliminated, but resources can be structured to address the greatest risks.
- NIST only identify information systems not control systems. Need to merge the two. CIP missing some of the NIST components.
- Conformance and compliance works well when you have check box spec system.
- Risk management may be what is needed to be done- but as a standard for compliance. Will be difficult to map up the two.
- Is there another tool to promote risk management other than a compliance approach?

5. Risk Assessment and Resource Implications

- Risk assessment done in federal sector by independent organizations. E.g. Iowa labs. It is an iterative process, like maintenance on car. Annual basis sometimes quarterly. Constant tweaks. Continuous improvement.
- The primary goal of the assessment process is impact analysis.
- We know the assets we need to protect. Are we mitigating the right risk for the right asset. Most valuable threat info (comes best from locally).
- It might be useful for INL or similar group to develop a risk assessment model for the industry, specifying what requirements actually are mandatory.
- In Florida, came up with "Risk = Impact divided by level of effort to accomplish the bad deed." From there they graded the risk levels of different deeds. A ratio (picked 1.0 threshold below which standard protection). Kept applying assets and compensation measures until risks went low. Critical assets review- risk assessment methodology.
- Risk assessment- grading security to the assets we have to take care of. Not sure how it has to work, but there is got to be a way to do it.

- Risk management and conformance – if outcome based standards with a risk management approach you can build a conformance model around that. Not always mutually exclusive.
- If the risk assessment framework were adopted, would it be a significant resource burden on the industry? Yes, it does take lots of resources to go through the FISMA exercise. CIP is narrower applying only to critical asset and cyber asset.

6. Component-Based Systems Approach

- Does a systems based approach vs. a component-based approach make any difference? More risks with certain components. Not adding or getting out of anything by using the NIST standards. Could probably modify the framework to deal with critical components.
- The SDT can modify anything in the NIST if it accurately assesses the risk of each component across and within the system.
- Component based vs. system based? Take the framework concepts and not the literal framework, we might have the opportunity to focus on what really needs protection. Give the industry appropriate, reasonable and achievable control and where they are given the options. This may present a challenge for auditors and the auditing process, but this may be the right step to take for the industry.
- The control system mechanism requires protection. Limiting the focus to "critical assets" necessarily overlooks areas of the control system that are essential but miss the target for receiving protection.

7. IT and Control Systems

- The overall issue is conventional IT vs. control systems. Before interconnection, no problems
- Opportunity: continue treating control systems as special, and build accordingly
- Alternative: emphasize reliability & resiliency, w/ chance to lead industry:
- The conventional IT environment has been geared to accept occasional outages as a cost of doing business, but that approach is not acceptable for control systems
- There is a "corporate IT" and "power system IT"; effective management and change control

8. Levels of Risk- "One Size Fits All"? NIST and CIP

- The fundamental problem with CIP that the SDT should address is the one size fits all in terms of critical cyber asset. There isn't the high, medium low judgment made in the NIST framework. It will be important for the industry to invest money and staff into focusing in on most important (i.e. high).
- Don't throw the CIP standards out and plug NIST in wouldn't work. Because it comes from a IT background not from a power plant control systems and control centers. What constitutes a cyber threat pushed out to specific equipment. Gap needs to be addressed in NIST and one size fits all in CIP needs to be addressed.
- The CIP standards effort tried to make it work otherwise. Don't need to throw all out the CIPs to address levels of compliance or types of equipment.

- We need lots of works on levels, controls. Try to preserve the industry investment made while making our existing framework better.
- Auditors may need to consider "appropriateness", perhaps. The current approach of CIP standards w/ all or none/one size fits all is not working.

9. **Compliance and Audit Concerns**

- In a compliance environment, more prescriptive directions for the NIST framework may be needed to facilitate auditing.
- FISMA and NERC amount of penalty associated with NERC standard. Doesn’t exist in NIST framework. Compliance environment with flexibility-
- SDT members offered to continue to lend the Federal lessons learned from implementing NIST and surviving numerous audits to the SDT. It has been an eye opening experience.
- Some federal entities are not subject to NERC sanctions, but there are implicit sanctions for them—appropriations lacking, or rate payers who are subject to the penalties for entities that are self supporting.
- Auditing community needs re-educated; they're typically in a checklist mentality because of other NERC Standards. Without the technical knowledge, they can't adequately determine whether efforts adequately address potential vulnerabilities in the cyber area.
- Conformance & compliance work well w/ a specific standard (pass/fail checklist); for cyber security. If risk management is the approach, another tool is needed besides conformance to compliance.
- What's needed isn't a "culture of compliance"; what's needed is a “culture of security.”
- NIST standards are not unlike others and audits are possible.
- FERC is concerned about the quality of what an entity does; it's not just checking off an item on a list.
- On audit issue, whichever route we take, the biggest culture change will be in the auditor community. Checklist mentality. Cyber requires analysis of what have you done. If they don’t have technical knowledge or working with that mindset.
- “Defense in depth”- filtering wall, firewall have BS. Can have those all and not have a secure architecture.

C. **Risk Management- Key Concepts and Questions**

The facilitators asked Kevin Perry to draft some strawman statements and questions to serve as a strawman for the SDT’s consideration. He introduced the statements noting it provides an overview of the statement of the current methodology a problem statement for the SDT’s consideration followed by 8 critical questions regarding risk management.

1. **The Current “Consequence-based” Assessment Methodology Draft Statement:**

The industry focuses on the facility (asset), employing a "consequences-based" assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:

- Those that are essential are declared to be Critical Assets.
- We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

Acceptability Ranking Scale	***4*** *= acceptable, I agree*	***3*** *= acceptable, I agree with minor reservations*	***2*** *= not acceptable unless major reservations addressed*	***1*** *= not acceptable*	***Avg.***
12-5 rank	**16** (13 + 3)	**0**	**2**	**0**	**3.9 of 4**

Comments before ranking

- Review of current process for assessing critical assets & corresponding CCAs.
- Focus on critical facilities/assets begs the issue of dynamic systems (e.g., flowgates)
- Industry could easily be "cherry picking" what they want to protect—the systems, related cyber systems. As a result, quality of review may vary
- An ESP doesn't address trusted path that crosses it (e.g., VPNs). A potentially vulnerable/out-of-scope system then has unrestricted access inside the perimeter.
- "All or nothing": there are no gray areas; a system either has to follow all CIP requirement or none.
- The "as is" statement describing the current methodology isn't accurate; by saying that non-critical assets are exempt from CIP Standards in the current scenario overlooks processes and activities that some have used to address situations such as those used in the example.
- The statement is accurately describing the situation that currently exists.
- The team needs to develop standards that can be audited against; there are various ways to accomplish that. The CIPC effort to develop guidelines for identifying critical assets has generated a lot of comments & won't be finalized for several months. However, whatever we create needs to align with the guidelines or vice versa.

Comments after ranking

- **2=** Don't agree with statement. CIP standards isn't a system approach. However don't see that CIP excludes a systems approach. Took an assets.
- 2= concern about the phrase "to the exclusion of pretty much everything else."
- Reason focus is on the critical assets is because NERC charge to deal with BES. Make sure all critical assets protected. This statement can't be right if we really think about what NERC's charge is.
- Standards say we can exclude. Drawing the line not in CIP. We exclude them from the CIP standards. Only requirement for maintenance. Logging at access point.

2. A Draft Problem Statement with the “Consequences-Based” Assessment Methodology

Kevin Perry presented the following problem statement as a strawman for the SDT’s review and consideration.

The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**16** *(14 + 2)*	**5** *(2 + 3)*	**0**	**0**	**3.8 of 4**

SDT Comments

- None

(b) The industry may be “cherry-picking” the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**9** *(6 + 3)*	**5** *(3 + 2)*	**5** *(5 + 0)*	**1**	**3.1 of 4**

SDT Comments

- Not related to this approach- accept gaming is part of the deal and move on.
- Not a problem statement for standards. This is part of implementation statement for the solutions.
- This implies industry is dishonest in “cherry picking.” Not necessarily the case.
- Should delete or reword this as a part of the problem statement.
- The "cherry picking" issue isn't primarily driven by a desire to not protect systems, but to make them exempt from CIP because of sanction issues

- **2nd Draft E.g. (b) Some in the industry may be ~~“cherry-picking”~~ selecting the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment based on economic vs. security considerations.**

(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**5 + 1**	**6 + 2**	**2 + 1**	**1**	

SDT Comments

- Doesn’t necessarily exclude. This is matter of interpretation.

(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 SDT rank	**17 *(13+4)***	**1**	**0**	**1**	**3.8 of 4**

SDT Comments

- When ever you have a perimeter, it is protecting your assets.
- Is this a problem
- Other issues to consider: are we addressing facilities? What are "systems"?
- Focus perhaps should be on functions vs. assets.
- The current approach focuses too much on "how we affect the national grid"; instead, entities should be looking at their own mission—what do they need to do to protect themselves? The result of that effort would lead to protection of the BES, in a manner more inclusive than the current approach. Using the national grid as the criteria allows too many loopholes to applying the standards.
- The definition of "critical assets" needs to be limited to physical assets. By bringing in the logical components would increase the complexity of identifying critical assets in another context (e.g., physical protection standards that might be developed in the future).
- These standards shouldn't be focused on Critical Assets; the cyber issues ought to be the priority.
- The SDT shouldn’t overlook the interest shown by Congress, and the promise to take action if industry doesn't respond in a timely or adequate manner. The input to the NOPR by a couple members of the committee was historic and unprecedented. The SDT needs to take that issue seriously.
- The focus is cyber security engineering, not electrical engineering.
- Is the current definition of "cyber asset" in the Glossary accurate & acceptable?
- Kevin Perry sent this to members over night: Definition of Computer System and Control System
- Definition of Computer System (http://www.webopedia.com/TERM/C/computer_system.html):
- “A complete, working computer. The computer system includes not only the computer, but also any software and peripheral devices that are necessary to make the computer function. Every computer system, for example, requires an operating system.
- Definition of Control System (DHS Catalog of Control Systems Security: Recommendations for Standards Developers): ‘A set of hardware and software acting in concert that manage the behavior of other devices.”

- Maybe can be added to the glossary and added to the definition of Cyber Asset. For example: Cyber assets include Computer Systems, Control Systems, programmable electronic devices, and communication networks including hardware, software, and data.
- Current NERC Glossary definition of Cyber Asset: "Programmable electronic devices and communication networks including hardware, software, and data.") His concern: the focus is on "the box", and an integrated system may not adequately be addressed.
- The existing taxonomy resulted from the historic focus on power engineering & bulk electric system reliability. Otherwise, a bottom-up approach would result in application of the standards to areas outside FERC's jurisdiction: market systems, etc.
- Be clear about "cyber asset" definition (e.g., data?).
- Don't overlook who our audience is.

D. Risk Management and CIP 002

1. CIP 002 Goal

The discussion regarding risk management led to a discussion and testing of a goal statement for CIP 002.

SDT Comments before Ranking

- What are we trying to accomplish w/ CIP-002? What is it's intent/end goal? The intended outcome?
- One possible answer: It's to identify cyber assets that need to be protected (& to what level—Mike Winters)
- What is the best way to identify those cyber assets/the best way to get there? [e.g. FDIC approach]
- By focusing on these two questions, we address the real needs and also satisfy the outcome focus that Mike Assante described this morning.
- The existing taxonomy resulted from the historic focus on power engineering & bulk electric system reliability. Otherwise, a bottom-up approach would result in application of the standards to areas outside FERC's jurisdiction: market systems, etc.
- Be clear about "cyber asset" definition (e.g., data?).
- Also critical to be considered is compromise of assets vs. loss of assets. An instance of malicious compromise of assets might be more damaging than its loss.
- The SDT shouldn’t overlook who our audience is.
- Disparity between use of terms "bulk power" and "bulk electric?” The definition in FERC Order 693 clarifies that.
- “Dueling risk assessments.” Id critical assets, then cyber. Risk of compliance second. Avoid that. Need is protection of system not just compliance.
- Understandable enough to see real goal is protection and compliance is a side effect not a goal.

The following CIP 002 goal statement was offered for ranking:

The goal/intended outcome of CIP 002 to identify the Cyber Assets (i.e. Programmable electronic devices and communication networks including hardware, software, and data, NERC Glossary) that need to be protected and to identify the level of protection.

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-5 rank	**16** *(15 +1)*	**4** *(3 +1)*	**0**	**0**	**3.8 of 4**

SDT Comments after Ranking

- Minor Concerns: Some felt that CIP 003 should only identify the CCAs but not go into the level of production.
- The SDT's key task is to identify what is the best way to get there.

2. What Should be the Framework for an Inventory of Cyber Assets?

SDT Discussion Points

a. Overall

- Key questions:
  - Are we getting to the inventory level we need to do under CIP's?
  - How do we set up a process that removes as much as possible that are not essential or critical?
  - How do we conduct the inventory?
  - What is the scope necessary for considering the protection of the infrastructure? To what level do we have to protect our "lifestyle"? (goes to SDT)
- Perhaps have entity initially catalog the cyber assets they use to support environment, then look at those assets from the perspective of how their loss, compromise, etc. would impact the BES
- Mindset problem in industry- interconnectivity and solve problem by changing. This go beyond communication and education.
- CIP 002 how do we apply the inventory framework. How well does it apply in that setting?
- Support the need for inventorying your assets. When you are identifying cyber asset using to control your generation, transmission, coordination centers. "Need to look at who is talking to me."
- Got to do inventory. How you do it is another issue. From a system point. Put arms around the outer limits. There was a clear concept with the first drafting team. We have to acknowledge that you have to know what you have in order to know what and how to protect. In future more routable protocols will produce more attack vectors.

- This is an engineering problem- critical asset facilities, applying engineering principles. Cyber security is not a physics problem. Can't apply the same principles. Developed a risk assessment methodology for 2 control centers. I.d. the 7 filtering criteria for determining the critical cyber asset. Easier today CMBB/ ITELL allow you to do the inventory.
- Will that approach address FERC's concerns?
- Concerns about "cherry picking" that removes things in the purview of CIP. Don't want in there simply because the sanctions threat. Whether this is the purview of NERC or not with the logging process. We do this now at a very high level. If someone can conclude that you can leave off your control system, that is just plain wrong.
- President Sergel's testimony: Characterized CCA as a priority-setting process. However it appears that entities in the industry are using it to identify what is in scope.
- Agreement that there needs to be a risk framework from a control system perspective.

b. Inside-Out Approach

- Good idea to use "inside out" approach
- Identify assets according to the areas they impact
- Go from the inside view inventory and get up. Then how to get auditable compliance. Not lots of confidence there are other options to test.
- Initial focus on cyber systems is logical and valuable. However law on BES vs. BPS differ; BPS is more expansive
- Would this approach lead to very few individual assets that actually would be covered by standard?

c. Systems View

- Needs to be viewed from aggregated view of systems
- What should the system look like- what is the vision?
- Need to know what's there; i.e., inventory
- There are systems that seem obviously critical from a common sense perspective, but fail to appear on lists; the risk assessment process is broken. An electrical engineering point of view is not working
- Mis-configuration is a major problem- systems management on configuration. Problem may be in the field organizations not in the data centers. Supports the idea of taking inventory. Find where it is. What is the outer limit of the system we are operating.
- There are many systems that are used for non-BES processes that would muddy the
- Critical to consider cyber systems and impact on other systems.
- Should market systems be covered by CIP? Taking information and sending instructions.

d. Protection Model

- If we were to devise an approach of a "protection model" that fit with the engineers' mindset, it might be a better way to reach them, teach them and satisfy the needs.
- Industry at large- understand operations thoroughly. Down to an art. Others know how to plan things, same tools with different models. What we don't have, is a protection model. We can use the same tools with a different set of models to figure out what we need to protect.

e. **Scope**

- If we start inventorying cyber assets- everything in north American grid with a chip in it? If you do at that level, you will have few cyber assets. We have to bump this up to a system level vs. a cyber assets level. Define and do it at that level. Need to look at aggregated points of control.
- Critical asset- 2 things. Protection critical to electric sector and then cyber security.
- Why should we inventory everything initially? Lot of systems that don't and won't have an impact on the BES.
- At what level do we assess what is on our inventory? Individual asset level or a system.
- Clarify what is the scale of inventory- not implying we don't need to do. Not ESO but ERO, write reliability standards.
- Not every cyber system is under the tent. Need to define the filtering what is important/not importance (FERC wide span of control etc.)

f. **What Assets Included?**

- Not necessarily everything in data center would be included
- Pure, raw, means of production are the key assets to be managed (also the approach original drafting team followed)
- IP-based assets are going to increase
- Problem is not data centers, but field organizations
- Need to protect the control system mechanisms.
- "Criticality of equipment"-- prioritizing how we go after the issue.
- Take an inventory; find where things are, what's the outer limits of systems that are operating
- One device in the substation that can't talk to anyone else will still need protection.
- Even if it's painful, it needs to be done
- Can't do anything unless you have an inventory- boxes and connections.
- Problem with going out and finding all assets- shouldn't be dealing with things outside those critical to the BES. To what level is it required. Identify a second tier level.
- Identifying negative potential impacts of software. The more subtle the error implemented, is a higher impact than a blue screen. Methodology to protect against.

g. **Real World Examples**

- Real world examples demonstrate the need for inventorying assets, better controlling systems & understanding dependencies. Better defined guidance for priorities is essential
- Similar approach for guidance for the AMI security task force. Domain based analysis. Attacker may go for something trivial vs. valuable and then hop-over. Draw domain around things. Use tools to define domain.
- Three legs of security- "availability" is the third leg. E.g. Southern-- Nuclear plant had an incident. Software on a business network. Communication. Engineer installing update on business system, didn't know it would affect the other system. Fixed.
- Look at incidents at Duke a few years ago. In the Florida incident, can't get a clear line of whether distribution or generation as the source of the threat.

h. Inventory and Compliance

- CIP 1- came up with an auditable framework. Creative way to make this a system to be auditably compliant. Can't model malicious control. PSSC tool leads to gross underestimating of cyber assets. Will have to go to a large set.
- CIP wasn't designed to preclude NIST framework to do your procedures. CIP is the auditable part. That's how the can be utilized and pulled together.
- Manage to compliance vs. cyber assets. N-1 is a part of the problem. Need to tie to something bigger than that. Come up a way to model more than N-1.
- Some of NIST is mandatory. Consider 800 standards. Issue of compliance was dealt with FISMA
- Current auditing in this sector is focused on checklist- dialogue needed- what are you trying to do, what means you have used, how effective. Talked about "quality" of what you did in terms of audit.

3. Draft SDT Inventory Statements

Following the inventory discussion, one member proposed testing SDT support for the following inventory statement:

a. Draft Inventory Statement

Inventory your cyber assets directly related to the operation of your registered NERC functionality:

- Apply a risk methodology to assign a level.
- Apply distinct controls according to the level.
- Inventory for each cyber asset should be: device + o's + function + firmware level.
- These attachments will be critical for patch management and CIP 007R1 testing.

Acceptability	*4 = acceptable, I*	*3 = acceptable, I agree with*	*2 = not acceptable unless major*	*1 = not*	*Avg.*

Ranking Scale	*agree*	*minor reservations*	*reservations addressed*	*acceptable*	
12-6 rank	**2** *(1 + 1)*	**6** *(3 + 3)*	**8** *(7 + 1)*	**4** *(4 + 0)*	**2.3 of 4**

Comments from SDT members finding the statement unacceptable or with major reservations:

- SDT member suggested that the above does not take into consideration of the reliability of the BES sufficiently.
- Need to start with Critical Assets, not devices.
- The starting point of the inventory was too broad; there may be a way of identifying the functions of the devices and including only some, but not all.
- Another member believed that the only important considerations should be only identification of the devices and the function of the devices;
- Add a new bullet that addresses the interconnection of the devices.
- FERC staff stated that the above approach moved in the right direction along with a way to identify other systems such as market systems where appropriate.

b. Draft Inventory Systems Statement

Following the first statement discussion, another SDT member proposed testing support for the following inventory statement:

> **Identify the applications and computer systems within the Industry Controls Systems or information systems as well as the networks within and interfacing with the ICS. The focus should be on systems rather than devices, and should include PLCs, DCS, SCADA, and instrument bases systems that use a monitoring device such as an HMI.**

Acceptability Ranking Scale	*4 = acceptable, I agree*	*3 = acceptable, I agree with minor reservations*	*2 = not acceptable unless major reservations addressed*	*1 = not acceptable*	*Avg.*
12-6 rank	**0**	**9**	**6**	**5**	**2.2 of 4**

Comments from SDT members finding the statement unacceptable or with major reservations:

- One SDT member believes that lack of specifying impact on the BES or BPS made the above unacceptable.
- the bottom up approach is not an acceptable approach.
- Another member believed that the impact profile of the entity should be considered in order for any proposal to be thorough.
- In response to an SDT member question, FERC staff stated that they have no limiting agenda. FERC through its order indicated it wants all of the systems protected to some degree and they like the framework that allows the entities to properly protect the systems as opposed to the CIP systems which are black and white. Under CIP if an asset is not designated as 'Critical' under the current regulations, no security or protection is required. FERC finds this approach lacking. However, FERC staff agreed that not everything should be protected to

the highest level. The assets that really are important should be protected at the highest level; however, nothing should be ignored.

SDT Discussion Points

- Start with a more inclusive view of all these devices. 002-R3 called out now some devices. Attack vectors.
- General concept of inventory of the devices- what are the appropriate filters.
- If we are called to testify- can we respond that our standards process is ensuring we are protecting the BES.
- Why are we here? Because there is inadequate IT life cycle management and power system IT--fragmented within. Are we good stewards of our company's assets and devices used?
- Everything should be inventoried- in corporate IT or power system IT. Reluctant to use IT but call it power system IT. Inadequate change management and loss of control
- Do it by design and explicit management decision. Doing a little bit of "greenfield design" here. Look at all cyber assets. Now with your full inventory.
- "It is all" IT 101- need to know what you are managing in your Skada.

E. Phase II Going Forward Proposal

Following the lunch break, the chair announced that Jackie Collett and William Winters had agreed to draft two "straw" documents to help move the Team forward on the Phase 2:

- Jackie Collett will start from an attempt to protect the best of what exists with the current CIP and incorporate NIST concepts/features.
- William Winters will start with the NIST framework and incorporate the best of the CIP into it.

SDT Advice to the Team Authors

- Authors agree to post to the SDT list
- Produce a workflow chart- business process management flow. Inputs/ outputs.
- Be as visual as possible
- All should read the House Committee's comments on FERC NOPR for CIP standards *(See Appendix #10)*

V. NEXT STEPS AND EVALUATION

A. SDT/NERC Phase 1 Webinar — December 16, 2008

NERC staff presented some information and the SDT discussed the industry "Webinar" on the Phase I SDT products.

- Time/Date: December 16 from 11:30 until 1 p.m. will be the Webinar on the topic of Phase I version of revised CIP.

- There will be a Standards Committee meeting that date.
- Dave Taylor will ask that the Committee listen to the SDT Phase I Webinar.
- SDT members should mark this date on the calendar.
- NERC will be putting out an press announcement on this next week.

The SDT then discussed the presentations for the Webinar:

- The emphasis should be on why we're doing what we're doing, give presentation and allow questions.
- Provide & explain information from the Phase 1 Comment Form.
- New asset implementation plan needs thorough explanation for industry.
- Mention why Phase I being done to begin with, draw attention to government scrutiny that we're receiving.
- Mention the new Congressional Cybersecurity Caucus that's beginning, point to FERC order requirements. Note why a phased approach was taken by the SDT and why we are proposing to take action now.
- Michael Peters agreed to prepare and provide background information.
- The Chair, Vice Chair and Scott Mix will present.
  - Jeri Brewer- 10 minutes on the Background reasons
  - Scott Mix - Actual Changes
  - Kevin Perry - Technical Feasibility Exception
  - Scott Mix - Schedule (near the end)
  - NIST - framework and how it applies in this scenario
- Note that there will be some Canadian government interest in issue. Need to follow-up needed to determine extent and whether it should be addressed.

B. Review of Phase I Schedule

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

- *December 16 — 11:30 a.m.–1 p.m., NERC Webinar on Phase 1*
- **January 7–9 SDT Meeting, Phoenix, AZ** ½ / 1/½ day format. Wednesday through Friday
- January 15 WebEx meeting
- January 21 WebEx meeting
- **February 2–4, 2009 Meeting in Phoenix, AZ,** ½ / 1/½ day format. Monday through Wednesday
- **February 18–19, 2009 Meeting in Boulder City, NV**
- February 25, 2009 WebEx meeting
- **March 10–11, 2009 Meeting in Tampa, FL,** 2–day format
- March 18, 2009 WebEx meeting

- **April 14–16, 2009 Meeting in Charlotte NC,** ½ / 1/½ day format. Wednesday through Friday
- March 18, 2009 WebEx meeting
- **May 13–14, 2009 Meeting in Dallas TX,** 2–day format
- June, WebEx meeting
- **June 17–18, SDT Meeting, Location TBD,** 2–day format
- June, WebEx meeting

C. January Meeting Agenda Review

NERC announce that the next meeting will take place in Phoenix at an Arizona Public Service Corporation conference facilities and will be a ½ day/1 day/ ½ day format. The proposed agenda items will include:

- Organizing to review and answer industry comments that have been received on the posting of Revised CIP standards from Phase I
- Finalize the SDT input to the NERC Technical Feasibility Exceptions white paper
- Time permitting, continued discussion of the CIP 002 approach to assets in scope for Phase II reviewing papers from Jackie Collett and William Winters.

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

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

What worked?

- Meeting in Washington, DC and exposure to Congressional perspective
- Appreciated being tagged onto the NERC CIPC meeting to allow others to participate as well as participation by NIST, Congressional committee member, etc.
- Good sound system.
- Appreciated the debate and the breadth of wisdom knowledge on the team.

What could be improved?

- Appreciate everyone have a chance to voice decisions. However sometimes we are saying the same things and repeating thoughts. Facilitators should try to close off open-ended discussion more quickly and move forward towards resolution.
- Place flip charts higher.

Meeting adjourned at 2:15 p.m. on Friday afternoon.

Appendix # 1 — Meeting Agenda

Washington, D.C. 20005

Thursday, December 4, Day One Agenda

1. 8:00 Opening Remarks - Jeri Domingo-Brewer, Chair & Kevin Perry, Vice Chair
   a. Welcome — announcements, logistics
   b. NERC Antitrust Compliance Guideline
   c. FSU/CRC review of last meeting and adoption of November 12–14 meeting summary
2. 8:15 SDT Organizational Issues: Review of Adopted Consensus Procedures
3. 8:30 NERC Presentation and Discussion of Phase I Communications Plan
4. 9:00 Technical Feasibility Strawman, Review and Refinement
5. 10:00 Break
6. 10:15 Technical Feasibility Strawman, Review and Refinement
7. 12:00 Lunch — working (return to meeting at 12:45PM ET)
8. 12:45 Summary of Phase II Concept- Next Steps
9. 1:15 Potential Application of NIST to CIP-Background Briefing and Discussion
10. 3:00 Stretch Break
11. 3:15 Risk Management — Conceptual Approach
12. 5:00 Recess

Friday, December 5, Day Two Agenda

13. 8:00 Opening, Review of Day One Results and Day Two Agenda — Jeri Domingo-Brewer, Chair & Kevin Perry, Vice Chair
14. 815 SDT Organizational Issues *(TBD)*
15. 8:30 Review and Further Refinement of Technical Feasibility Draft
16. 10:30 BREAK
17. 10:45 Final Review and Adoption of Technical Feasibility Draft
18. 11:15 Continue Review of Risk Management Approach, NIST and CIP 002-009 — Approach
19. 12:00 Lunch — working (return to meeting at 12:45 p.m. ET)
20. 12:45 Implications from Risk Management Discussion for CIP 002
21. 2:30 Review of meeting schedule and drafting assignments
22. 2:45 Next Steps and Evaluation
23. 3:00 Adjourn

Appendix # 2

Project 2008-06 Cyber Security for Order 706 SDT Attendees List

Washington D.C.
December 4–5, 2008

Attending in Person — SDT Members

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

SDT Members Attending via WebEx and Phone

1.Phillip Huff	Arkansas Electric Coop Corporation
2.Kevin Sherlin	Sacramento Municipal Utility District *(Day 2)*
3. Bryan Singer	Kenexis Consulting Corp.
4.Jonathan Stanford	Bonneville Power Administration
5.Michael Winters	Hydro One

Attending — Participants *(in person and by phone and WebEx)*

Chuck Abell	Ameren *(in room Dec 4, on phone Dec 5)*

Joseph Baxter	Associated Electrical *(by phone Dec 5)*
Jim Brenton	ERCOT *(in room Dec 4 and Dec 5)*
Markus Braewole	ABB *(by phone Dec 4)*
Steve Breziwa	WAPA *(by phone Dec 4 and Dec 5)*
Mike Fischette	Lansing Board of Water and Light *(by phone Dec 4)*
Jerome Farqumarson	Burns and McDowell Engineering *(in room Dec 4 and Dec 5)*
Brian Harrel,	SERC Reliability *(by phone Dec 4 and Dec 5)*
Darren Highfill	EnerNex Corporation *(in room Dec 4, on phone Dec 5)*
Steve McElwee	PJM *(In room Dec 4, by phone Dec 5)*
William McEvoy	Northern Utilities, *(In room Dec 4)*
Austin Montgomery	Salisbury Institute, CMU *(in room Dec 4, on phone Dec 5)*
Mike Peters	FERC (*in room Dec 4 and Dec 5)*
Matt Schnell	Nebraska Public Power District *(Dec 5 on phone)*
Mark Simon	Encari, *(by phone Dec 4)*
Michael Toeaker	Burns and McDowell Engineering *(by phone Dec 4 and Dec 5)*
Karen Yoder	First Energy *(by phone Dec 4 and Dec 5)*

Appendix # 3
NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

Appendix # 4

Below is a link to all of the documents reviewed by the SDT 706 Team during the full Team discussions in Washington D.C. as well as Phase 1 SDT Products:

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

Appendix # 5 — SDT Consensus Guidelines

Adopted Unanimously, November 13, 2008

The Cyber Security for Order 706 Standard Drafting Team (Team) will seek consensus on its recommendations for any revisions to the CIP standards.

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

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

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

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

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

Meeting Guidelines for Participants

Participants' role in meetings:

- Explore possibilities
- Listen to understand (Respect) (limit sidebar conversations)
- Be focused and concise. (Avoid repetition. No need to offer comments in "strong agreement.")
- Focus on issues, not personalities.
- Offer options to address others' concerns.
- No sidebars.
- If participating by phone, indicate who is speaking.
- If participating by phone, please use the mute button. **Do not** put the phone on hold.

Facilitators/Staff role in meetings:

- Assist the Chair and Vice Chair in helping the Team stay on task
- Help the group follow agreed upon ground rules
- Design the meeting and problem solving process in consultation with the Chair and Vice Chair
- Facilitate discussion participation of the Team and other participants
- Prepare agenda packets and reports

Consensus Building Techniques

- **Brainstorming** (green light thinking – not judgmental) At certain points, the facilitator may ask the group to suspend judgment and get ideas onto the table before debating.

- **Name Stacking in Team Discussions** (use of name tents to seek attention)

- **Acceptability Consensus Ranking Scale**
  - Use a consensus acceptability scale to help focus discussion and test support in reviewing substantive issues.

- Use to guide and focus discussion and as a poll to see where the Team stands, not used as a voting mechanism.
- Must be prepared to offer refinements and suggestions to address serious concerns.

4 = Proposal is acceptable as it is
3 = Proposal is acceptable; I can live with it but there are minor concerns to address
2 = Proposal is not acceptable. Proposal may be acceptable if the major concerns are addressed
1 = Proposal is not acceptable

o **Consensus Ranking Scale**

4. Comfortable—I support proposal as is ♥♥♥♥
3. Minor Reservations— I can live with this; but would like to see changes as follows♥♥♥ Be prepared to offer specific refinements or changes to address your concerns.
2. Major Reservations—I can't support this unless following changes are addressed to meet my serious concerns ♥♥ Be prepared to offer specific refinements or changes to address your concerns.
1. Fatal Flaws—I can't support this ♥ Be prepared to offer alternatives and options that would address your own as well as other's concerns.

o **Robert's Rules of Order and Facilitated Consensus Building Procedures**

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

Appendix #6
Technical Feasibility Framework White Paper, Scott Mix, NERC

December 5, 2008

Objective, Purpose, Executive Summary, and Background

The purpose of this whitepaper is to describe a proposed framework to address the Technical Feasibility exception provisions introduced in the cyber security standards (CIP-002-1 through CIP-009-1).

The proposed Technical Feasibility Exception process is modeled after the existing Self-report of Non-Compliance with Mitigation Plan process. These similarities are beneficial because it is anticipated that this Technical Feasibility process will be administered by the same staff at both the Regional Entity and ERO.

Definition of Technical Feasibility Exception:
A Technical Feasibility Exception (TFE) may arise when compliance with a requirement or sub-requirement under a CIP Reliability Standard is not technically possible, technically safe or operationally reasonable given the responsible entity's environment. A TFE may be invoked by a Responsible Entity only on a case-by-case basis within the Technical Feasibility Framework.

Application:
A Responsible Entity may invoke a Technical Feasibility Exception (TFE) to a NERC Reliability Standard requirement only where explicitly allowed by the language of a specific standard requirement or sub-requirement. Entities may file a Self-Report of Non-Compliance in cases (1) where they cannot meet the requirements specified in the Reliability Standard and no allowance for a TFE is requested or (2) where the TFE process requirements cannot be met (see FERC Order 706 paragraph 160).

Overview of Essential Elements:
Each TFE request must contain the following essential elements, as described in FERC Order 706, paragraph 222:

- Document mitigation steps.
- Document a remediation plan.
- Document a timeline for eliminating the use of the TFE unless appropriate justification otherwise is provided.
- Provide regular review of whether it continues to be necessary to invoke the exception.
- Document internal approval by the Senior Manager.
- **Document wide-area approval through the ERO's audit process.**

Additionally, the TFE process requires cooperation with the ERO to provide FERC with high-level, wide-area analysis regarding the effects of the TFE on the reliability of the Bulk Electric System. In other words, where a TFE is requested, the impact on interconnected assets must be considered in the development of a remediation plan. This may require coordination with one or more Responsible Entities prior to submission for approval.

In addition to the FERC-directed elements, the following steps are proposed:

- The request must reference the NERC standard and requirement for which the TFE is being requested.
- The "regular" review will be an annual review by the Responsible Entity, Regional Entity, and ERO.
- To facilitate cataloging and tracking, each TFE will be assigned a unique identifier by the Regional Entity that initially receives the TFE, during its review process.

Detailed TFE Process:
The TFE process described herein is based on the existing NERC Compliance Self-Report of Non-Compliance to a Reliability Standard. Each of the essential elements of a TFE report is described below.

The following elements are the responsibility of the Responsible Entity requesting the TFE:

- **Document the exception**
  Each TFE request must reference the specific NERC Reliability Standard requirements or sub-requirements for which the TFE is being requested[1].

  Each TFE request must include a description of the equipment, process, or procedure that prevents the entity from meeting the requirement and explain the reason for the inability to meet the requirement. The justification should focus on the impact to reliability that will result if the requirement cannot be met. Also included in this explanation may be a discussion of the impact of not complying with the requirement, or the impact of improperly literally complying with the requirement. This explanation may also discuss how other factors impact the TFE

[1] It is anticipated that future limitations on where TFEs may be implemented. These limitations will be implemented through modifications to the language of the standards. However, the immediate need for the TFE process requires that the process be developed in advance of these modifications. This proposed process can be implemented in a "field test" environment to allow the future specification of where TFEs may be requested, leading to modifications of the standards language during the next review and approval cycle. The determination as to whether specific requirements should be allowed or disallowed will be deferred until that point. These changes must include a discussion of operational and safety concerns, as discussed in FERC Order 706, paragraphs 178 and 182.

request, such as scarce technical resources, funding availability, equipment availability, etc.

A single TFE request may be associated with multiple equipment instances that share a common issue with regard to the request for the TFE. The issues, situations, mitigations and timelines associated with the TFE are assumed to be similar, and the approval process and impact analysis is expected to be the same.

- **Document and implement mitigating and/or compensating steps**
  Each TFE request must include a description of what actions the Responsible Entity has taken to mitigate, compensate, or lessen the impact of the vulnerability resulting from not being able to comply with the requirement(s) of the Reliability Standard.

  The Responsible Entity must demonstrate the implementation of the mitigating and/or compensating steps to the Regional Entity or the ERO upon request.

  For example, in standard CIP-005 R2.4, if a TFE is being requested for the lack of "strong procedural or technical controls at the access points to ensure authenticity of the accessing party," a mitigation measure might be to implement additional procedures to log all access attempts, more aggressively monitor those logs for unauthorized access, and provide a rapid response when an unauthorized access attempt is detected. In the same example, a compensating measure might be to install an extra in-line communications device to provide the strong authentication component, and force all access to go through the extra device. For purposes of meeting the intent of the requirement, either (or both) could be acceptable, but the chosen method would need to be documented as a mitigating or compensating measure on the TFE request.

- **Document and implement a remediation plan**
  Each TFE request must include a plan for resolving the issue being requested. The remediation plan may provide an extended (e.g., multi-year) plan, for example, to upgrade equipment to versions that are compliant with the Standards requirement, to allow for contract renegotiations, or to allow for regulatory amendment. Alternatively, the remediation plan may be to implement mitigating and/or compensating measures sufficient to protect the component until the equipment for which the TFE is requested reaches its natural end of life and is replaced with a compliant version of the equipment if such equipment exists at that time.

  The Responsible Entity must demonstrate the implementation of the remediation plan to the Regional Entity or the ERO upon request.

- **Document a timeline for eliminating the use of the TFE unless appropriate justification is provided**

Each TFE request must include, as part of its remediation plan, a timeline for the elimination of the need for the TFE. There are no specific requirements for the timeline: it may be short or multi year; it may be detailed or general. It must, however, effectively communicate the Responsible Entity's commitment to resolving the TFE in a manner consistent with maintaining appropriate cyber security and Bulk Electric System reliability.

In some cases, there is no possibility for eliminating the TFE. For example, providing a completely enclosed boundary around a circuit breaker containing an embedded controller that may be classified as a Critical Cyber Asset is not possible. Also, completing personnel risk assessments prior to providing access to Critical Cyber Assets may not be possible during restoration activities after a natural disaster. In such cases, the timeline cannot include a definite end date; therefore, the timeline discussion must include a justification for not having an end date, in addition to specifying that there is no end date. Note that absent a compelling argument for maintaining the TFE request, the Responsible Entity is expected to become compliant with the Reliability Standard requirement upon replacement of the equipment necessitating the TFE request (see FERC Order 706 paragraph 181).

In cases where there are milestones associated with a timeline, the Responsible Entity must show progress meeting the identified milestones to the Regional Entity or the ERO upon request.

- **Provide regular (annual) internal review of whether it continues to be necessary to maintain the exception**
  Each Responsible Entity requesting a TFE must at least annually provide documentation, subject to an audit, that (1) the TFE remains necessary, (2) all remediation plan steps requested by the TFE remain in place and are effective, and (3) any timeline milestones for the elimination of the TFE are on schedule for successful completion of the remediation plan. The documentation must be provided upon request to the Regional Entity and ERO, subject to audit (see also "Sensitive Information" section below).

- **Document internal approval by the Senior Manager**
  The TFE request must be signed and dated by the Senior Manager[2] appointed per Requirement R2 of *CIP-003-1 – Security Management Controls* (no delegation allowed). The request must indicate that the Senior Manager has read and understands all of the components requested by the TFE. The TFE must be reviewed and approved by the Senior Manager at least annually based on the date of the initial TFE request. The Senior Manager must also review and document the progress the Responsible Entity is making toward completing the remediation plan timeline. All missed milestones must be approved by the Senior Manager and reported through the wide-area approval process described below.

- **Submit TFE to Regional Entity (and subsequently to the ERO)**
  Notice of each TFE, when complete and approved by the Responsible Entity's Senior Manager, must be submitted to the compliance office of the appropriate Regional Entity to catalog.

  In each instance, the Responsible Entity must make available for review the details of the TFE, including background and justification for requesting the TFE. Failure to make the TFE details available upon request to authorized representatives of the Regional Entity or ERO, subject to the protection requirements described below, will result in automatic disapproval of the TFE.

  Note that 'submitted' does not necessarily mean that the full TFE documentation is physically or electronically transmitted to the Regional Entity or ERO; it may mean that only a notice of TFE is transmitted to the Regional Entity and ERO.

  The annual re-approval by the Responsible Entity shall re-submitted to the Regional Entity.

The following elements are the responsibility of Regional Entity and ERO:

- **Receive TFE submissions from Responsible Entities**
  Upon submission of the TFE to the Regional Entity, the Regional Entity shall assign a unique catalog identifier to the TFE for further reference. The Regional Entity will ensure that the TFE submissions are complete, and that sufficient information is included to allow the required approvals and analysis.

[2] The Compliance Monitoring and Enforcement Program (CMEP) refers to the approval entity as a Senior Officer. Since the CIP Standards use the term Senior Manager, it is used here. These individuals may be the same person for a specific Responsible Entity.

- **Annual review of TFE**
  The Regional Entity shall review the resubmitted TFE requests to verify that the re-submitted TFE remains valid. Any resubmitted TFE must be analyzed to determine if the TFE must be reapproved.

- **Document wide-area approval through the ERO's audit process**
  Each TFE will be individually analyzed and evaluated prior to approval by the Regional Entity. This analysis and evaluation will take into account all documented particular circumstances and justifications to ensure that the TFE request is valid, that the mitigating and/or compensating measures are appropriate for the TFE and the mitigating and/or compensating measures address the associated impact to the reliable operations of the Bulk Electric System. Only information included in the TFE request will be analyzed; if additional information is required, the TFE request may be updated by the Responsible Entity during the approval analysis and evaluation process.

  Upon receipt of the notice of TFE, the Regional Entity may need to visit the Responsible Entity to review the details of the TFE request in order to analyze and approve the TFE request.

  Included in the Regional Entity approval process is an analysis of the impact to Bulk Electric System reliability for the TFE request. This may require coordination with one or more Responsible Entities prior to submission for approval in addition to any analysis performed by the Regional Entity.

  Updates to the TFE, specifically including updates to the Responsible Entity's completion of milestones in the remediation plan, must also be submitted to the Regional Entity for wide-area approval through the ERO's audit process. Significant unreported and unapproved deviation from meeting the established remediation plan milestone dates may result in a finding of non-compliance with the requirements of the Reliability Standard (see FERC Order 706 paragraph 160).

  Following approval by the Regional Entity, notice of the TFE must be submitted to the ERO for its cataloging and for input into the wide-area analysis, following a similar process.

  Note that separate approval analyses and evaluations will be conducted by the Regional Entity and the ERO; therefore, the TFE request may need to be updated during each review.

Good Faith efforts
Responsible Entities may assume TFEs submitted in good faith are valid and accepted until rejected during the review process, provided the submitted TFE is technically sound, complete and addresses the exemption. Any preliminary rejection determinations should be investigated to determine if the Responsible Entity could modify and resubmit its TFE request to satisfy the reason for the rejections.

Sensitive Information:
It is recognized that many TFE requests will contain sensitive information that must be protected against disclosure, including information that must be protected from Freedom of Information Act (FOIA) release for certain U.S. Government agencies. The Regional Entities and the ERO will work with the Responsible Entity to minimize the possibility of release, but must have access upon request to the TFE requests in order to carry out their regulatory oversight responsibilities. Similarly, the Regional Entity and the ERO will work with the Responsible Entity to ensure that personnel with proper clearances are assigned to the review. Note that inability to review the TFE request, regardless of reason, may result in the disapproval of the request. Information used in the TFE approval and analysis process shall be protected pursuant to NERC’s Rules of Procedure section 1500.

As discussed above, review of the TFE by the Regional Entity and ERO does not require that the Regional Entity or ERO take physical possession of the TFE documentation; an on-site review of the TFE documentation will, in many cases, suffice. Actions taken during the review will be mutually agreed to by the Responsible Entity and the reviewing party, and depend on specific legal requirements.

Post Approval Processes required by FERC Order:
Additionally, the TFE process requires cooperation with the ERO to provide the FERC with high-level, wide-area analysis regarding the effects of the TFE on the reliability of the Bulk Electric System.

The ERO, in conjunction with the Regional Entities, must provide a summary report to the FERC providing a high-level, wide-area analysis of the combined effects of all current TFE requests. In order to produce this report, the ERO and the Regional Entities must have appropriate access to the TFE requests from each Responsible Entity. In some cases, it may be necessary to conduct interviews of the individual Responsible Entities to determine the individual and combined impact of the TFE requests within that Responsible Entity, and to determine what wide-area impact, if any, the TFE requests represent in aggregate (see FERC Order 706 paragraph 221). Failure to cooperate with the ERO or the Regional Entity to provide such information upon formal request may result in the rejection of the TFE, and subsequent possibility of non-compliance with the Reliability Standard (see FERC Order 706 paragraph 160).

This wide-area impact analysis shall be re-conducted annually using the most recently submitted TFEs.

Appeals Process:
The appeals process for any TFE request that is rejected by either the Regional Entity or the ERO shall follow the existing Compliance Monitoring and Enforcement program appeals process.

Sample TFE Request Form Fields:
(A form will need to be developed)

Responsible Entity:

Entity Name:

NERC Compliance Registry ID Number:

Compliance Contact Name and Title:

Compliance contact Phone

Compliance Contact email

Technical Contact Name and Title:

Technical Contact Phone:

Technical Contact email:

Date of Technical Feasibility Request submission:

NERC Standard:

Requirement in Standard:

Justification for requesting a Technical Feasibility Exception:

Mitigation and/or Compensation taken:

Remediation Plan steps, milestones and timeline:
If no timeline is given, provide justification for not providing a timeline

Initial Internal Approval by Senior Manager or compliance Senior Officer
Name, title, Date of Approval:

Internal Annual Re-approval by Senior Manager if timeline is longer than one year or no timeline is given

Justification for continued re-approval:

Regional Entity Approval:

Regional Entity:

Technical Feasibility Exception Number (assigned by Regional Entity)

Regional Entity Approval Name

Regional Entity Approval Date

Regional Assessment of impact of Technical Feasibility Exception:

ERO Approval:

ERO Approval Name

ERO Approval Date

ERO Assessment of impact of Technical Feasibility Exception:

Appendix #7 — Phase II Assessment Criteria and Workplan Options

2nd DRAFT PHASE 2 OPTIONS ASSESSMENT CRITERIA

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

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

Phase II Work plan Options in Rank Order

(Identified and ranked by SDT November 14, 2008)

1. Address Risk management first then proceed with the rest

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

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

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

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

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

4. Start Over — in terms of a starting point

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

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Appendix #8 Risk Management Worksheet

The SDT Conceptual Approach Risk Management

NOTE: The following points and questions were developed by Kevin Perry to help focus the SDT discussion on risk management. The purpose of this discussion is to provide an initial consideration of important information, options and arguments regarding risk management.

The Current "Consequence-based" Assessment Methodology:

We focus on the facility (asset), employing a "consequences-based" assessment methodology to determine if the facility is essential to the reliable operation of the bulk electric system:

1) Those that are essential are declared to be Critical Assets.
2) We then determine the Cyber Assets essential to the operation of the identified Critical Asset and those become subject to the CIP standards to the exclusion of pretty much all else.

Acceptability Ranking Scale	***4 =** acceptable, I agree*	***3 =** acceptable, I agree with minor reservations*	***2 =** not acceptable unless major reservations addressed*	***1 =** not acceptable*	***Avg.***
12-5 rank					

A Draft Problem Statement with the "Consequences-Based" Assessment methodology

The problem presented with this approach is that:

(a) Given the dynamic nature of the transmission system, assets that are critical today might not be tomorrow, and vice versa.
(b) The industry may be "cherry-picking" the Cyber Assets to be protected, along with any collateral Cyber Assets that happen to be connected to the same network segment.
(c) The approach excludes all other Cyber Assets, including Cyber Assets that may provide essential data to the Critical Cyber Assets or may have a trusted relationship (communications path) that could be exploited as an attack vector. And
(d) Once a Cyber Asset is identified as either a Critical Cyber Asset or a collateral Cyber Asset within the Electronic Security Perimeter, all of the requirements of the CIP Cyber Security Standards apply, regardless of the specific Cyber Asset's importance to the reliable operation of the Bulk Electric System.

Acceptability Ranking Scale	***4 =** acceptable, I agree*	***3 =** acceptable, I agree with minor reservations*	***2 =** not acceptable unless major reservations addressed*	***1 =** not acceptable*	***Avg.***
12-5 rank					

Overview of Considerations and Key Discussion Questions

1. Should the current Critical Cyber Asset identification process continue without modification?
2. Should the concepts of the NIST Risk Management Framework be adopted in some form, allowing for degrees of importance and corresponding protection controls?
3. Should the same risk management approach be used for field assets (e.g. generation plants, substations) as are used for traditional datacenter environments (e.g. control centers)?
4. Should there be a distinction between Critical Assets and non-Critical Assets (facilities) or should Cyber Assets in all facilities be protected to some degree?
5. Should the Critical Cyber Asset identification process consider the interaction of connected Cyber Assets and the vulnerabilities therein?
6. Should all Cyber Assets at a Critical Asset (facility) be subject to at least a minimal set of basic cyber security standards?
7. How does the NIST framework concept of risk acceptance compare/conflict with the FERC Order 706 and could it work given the FERC's current position on the subject?
8. Should there be some consideration of the importance and potential impact to a Critical Cyber Asset/Bulk Electric System reliability when assessing compliance penalties? For example, if all Cyber Assets at a facility require compliance with at least a minimal set of security standards, should a compliance failure charged against an office PC be subject to the same penalty structure as a Critical Cyber Asset?

Should any of these questions be deleted, reworded or changed in regard to the order?

Are there any additional questions to be considered?

For each question:

- *What are the issues at play in answering this question?*
- *Any guidance or directives from FERC Order 706 that the SDT should consider?*
- *Any additional information needed to answer this question?*
- *Following the discussion of the questions above, are there any draft statements that should be ranked for acceptability? (4,3,2,1 scale)*

FERC 706 Background References

Regarding NIST:

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

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

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

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

Regarding Risk Management

253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposedDocket No. RM06-22-000 - 71 -to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO's discretion whether to incorporate such guidance into the CIP

Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.

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

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

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

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

258. As to Entergy's suggestion that the ERO provide a DBT profile of potential adversaries, the

ERO should consider this issue in the Reliability Standards development process. Likewise, the ERO should consider Northern California's suggestion that the ERO establish a formal "feedback loop" to assist the industry in developing policies and procedures.**85**

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

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

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

Regarding an additional guidance or reference document

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

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

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

408. The Commission agrees with FirstEnergy on the importance of flexibility in developing a mutual distrust posture, but does not see a conflict between the need for flexibility and what it is proposing, which is simply more guidance. More guidance will allow responsible entities to implement measures adapted to their specific situations more consistently and effectively. Additional guidance need not be included in a specific Requirement, but could be in the form of examples. We will leave it to the Reliability Standards development process and the ERO to decide whether some or all of the guidance can be contained in separate guidance documents referenced in the Reliability Standard. In response to Entergy, the Commission is not directing that the ERO establish a specific end result. Our concern is simply that responsible entities have guidance on how to achieve an appropriate result in individual cases, which can vary on a case-by case basis. We disagree that providing useful guidance affects the scope of the Reliability Standards.

502. In response to APPA/LPPC, the Commission clarifies that it does not intend to create an inflexible rule calling for redundant electronic security in all cases. While the Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process. This would include whether or not

the second security measure must be "on par" with the first. The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

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

547. In sum, we direct the ERO to modify Requirement R4 to require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years. The ERO should develop the details of how to determine what constitutes a representative system and what modifications require an active vulnerability assessment in the Reliability Standards development process. The revised Reliability Standard should contain the essential requirement that an active assessment must be performed at least once every three years. Based on the amount of guidance contained in the modified Reliability Standard, the ERO should consider at that time whether additional guidance should be provided in a reference document.

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

006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.

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

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

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

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

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

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

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

Appendix # 9

FERC 706 NOPR Response of House Committee on Homeland Security

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING) Docket No. RM06-22-000)
MANDATORY RELIABILITY STANDARDS FOR)
CRITICAL INFRASTRUCTURE PROTECTION)

COMMENTS OF

REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY

REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY

REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY
STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING) Docket No. RM06-22-000)
MANDATORY RELIABILITY STANDARDS FOR)
CRITICAL INFRASTRUCTURE PROTECTION)

COMMENTS OF

REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY

REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY

REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY
STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

I. INTRODUCTION

As Members of Congress, we are pleased to provide these comments in response to the Notice of Proposed Rulemaking (“NOPR”) issued in the above-captioned docket.[3] We support the efforts of the Federal Energy Regulatory Commission (“FERC”) to require the North American Electric Reliability Corporation (“NERC”) to develop modifications to the Critical Infrastructure Protection (“CIP”) Reliability Standards. However, we believe that the reliability of the nation’s bulk-power system (“BPS”) will be better protected by a cyber security standard that incorporates the additional security measures of National Institute of Standards and Technology (“NIST”) Special Publication (“SP”) 800-53 as applied to industrial control systems.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:
Jacob Olcott
Subcommittee Director and Counsel
Emerging Threats, Cyber security,
Science and Technology Subcommittee
Committee on Homeland Security

[3] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515
(202) 226-2616
(202) 226-4499 (facsimile)
Jacob.Olcott@mail.house.gov

III. BACKGROUND

The BPS of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people.[4] The effective functioning of this infrastructure is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever- present cyber risks that exist in the information technology world in addition to control system specific risks."[5]

The cyber risk to these systems is becoming increasingly dangerous. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the BPS, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[6] Since the release of that study, numerous unintentional cyber incidents – from the Davis-Besse power plant incident in 2003, to the Northeast blackout, to the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted.

But nothing quantified the intentional threat to the BPS quite like the experiment performed by the Idaho National Laboratory for the Department of Homeland Security. In September 2007, the Department disclosed that its researchers successfully destroyed a generator while conducting an experimental cyber attack. According to news reports, the attack involved a controlled hack of a replicated control system commonly found throughout the BPS.[7] The

[4] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.

[5] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.

[6] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.

[7] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007,

results of this experiment suggest that malicious actors could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure.

Clearly, intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the U.S. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.[8] This figure does not consider the negative societal or health ramifications that such an event would have on the American people.

The FERC proposes to approve a set of reliability standards to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. The FERC recently created an Office of Electric Reliability ("OER") designed to focus on the development and implementation of these standards for the users, owners, and operators of the grid.

Unfortunately, we believe the standards proposed by the NERC for adoption by the FERC do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. We are primarily concerned with five issues: 1) the limitations of CIP-002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures. The fact that our comments are primarily related to the first of the proposed eight standards should not be construed as support of the remaining standards, but demonstrate our deep concern with the implementation of CIP-002-1. We believe that the reliability of the nation's BPS would be better protected by a cyber security standard that incorporates the additional security measures of NIST Special Publication 800-53 as applied to industrial control systems.

IV. DISCUSSIONS OF MAJOR ISSUES OUTLINED IN THE NOPR

Though we applaud FERC's efforts and support many of its modifications to the NERC CIP Reliability Standards, we are primarily concerned with five issues: 1) the limitations of CIP-

from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[8] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures.

NERC's proposed CIP-002-1 requires an entity to identify its "critical assets" and "critical cyber assets" using a risk-based methodology. Identifying assets is arguably the most important step in the entire assessment process. With control systems becoming increasingly interconnected to each other, and also interconnected with corporate data networks and the Internet, many assets that were once thought to be isolated are now vulnerable.[9] As noted in the FERC Staff Preliminary Assessment, "because CIP-002-1 addresses the assessment methodology and process for identifying critical assets and critical cyber assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards."[10] However, if implemented in its present form, CIP-002-1 would not require responsible entities to comprehensively secure "critical assets" that could in fact have a significant impact on the safety and security of the United States.

The problem lies with the NERC definitions of "critical assets." NERC defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets."[11] "Critical assets" are defined as "facilities, systems, and equipment that would affect the reliability or operability of the BPS."[12] This is a conceptual mistake that fails to understand the importance of the reliability and operability of individual elements of the grid, which are essential to the delivery of power to the nation's critical infrastructure.

The BPS is an enormous, interconnected network that is both redundant and resilient, making the sole focus on "reliability" and "operability" of the grid as a whole inappropriate. Practically, there are several assets that would fall outside the scope of NERC's definition of "critical" which should not. For instance, although generation units serving communities locally regularly trip offline due to both unexpected events and routine maintenance alike, service to customers generally remains constant. This is a credit to the design of the greater grid, which is engineered to withstand these kinds of singular events.[13] Critical to providing power for

[9] Today, the existing "NERCnet" employed for inter-control center coordination arguably provides a direct link for hacker access to most utility control centers in North America.

[10] Federal Energy Regulatory Commission, *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, December 11, 2006.

[11] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.

[12] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.

[13] North American Electric Reliability Corporation, Transmission Planning Series Standards (TPL).

citizens, businesses, and other critical infrastructures, these units would not be defined as such because they would not affect the reliability or operability of the BPS itself. Similarly, individual substations may experience reliability problems, but unless the load shed exceeds a certain level of megawatts, it is unlikely that a single substation would be recognized as a critical asset under the NERC definition. Telecommunications equipment would also be excluded from the "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations.[14]

Finally, though it is impossible to argue that they are not critical to the safety and security of the U.S., distribution assets would be excluded because they are not essential to reliability of the BPS. Again, real world examples expose problems with this logic. Though the BPS was restored within days to the primary areas affected by Hurricane Katrina, it took some municipal water department pumps over a year to get back up and running because the distribution systems remained off-line. In a June 2007 incident, an outage in Tempe, Arizona, caused by the unexplained activation of the distribution load shedding program in the energy management system affected nearly 100,000
customers.[15]

It is easy to see that an intentional or unintentional cyber incident on the BPS resulting in the disability of any connected asset – from distribution control systems to telecommunications equipment – can have a significant impact on the nation's security. Every critical infrastructure in the country is dependent on the BPS: chemical plants, banks, refineries, hospitals, water systems, and military installations all rely on the effective operation in their region. Focusing on assets relative to the functioning of the grid as a whole misses the importance of each individual asset to the functioning of our society. Unfortunately, recognition of the major infrastructure dependencies on the BPS is entirely absent from the FERC NOPR. Though the NOPR suggests that FERC "will revisit this matter through future proceedings and with other agencies," it is difficult to understand why cross-sector dependencies on the BPS are not the main focus of this standards process.[16] To address this shortcoming, we suggest that every electronically connected asset be considered "critical," as failures on those systems could potentially cause cascading outages of the BPS that could affect every critical infrastructure associated with it.

We strongly support FERC's efforts to provide guidance on the content to be applied in the

[14] On June 20, 2003, NERC issued a lessons learned advisory about the "SQL Slammer Worm," a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic in early 2003. However, CIP-002-1 excludes telecommunications equipment because it is not a "critical asset."

[15] U.S. Department of Energy, Office of Electricity and Delivery Reliability, Infrastructure Security and Energy Restoration, "Energy Assurance Daily" (June 29, 2007), available at http://www.oe.netl.doe.gov/docs/eads/ead062907.pdf.

[16] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

risk-based assessment methodology and require that a senior manager annually review and approve the methodology. We do hope, however, that FERC will create a meaningful deadline for the issuance of such guidance so that it can be effectively promoted across the system. It is true that one singular methodology is probably not appropriate for all situations or entities, but FERC should define the acceptable characteristics of a methodology. While flexibility is important, allowing each responsible entity to craft its own methodology may lead to difficulties in assessing risk across the system. Explicit requirements will avoid a situation where neighboring utilities with the same equipment can have completely different critical cyber assets by virtue of their interpretation of the definitions. Ultimately, however, as long as a responsible entity uses a risk-based methodology focusing on the reliability of the BPS rather than the critical infrastructure end user, safety and security concerns remain paramount. We expect FERC will establish an expedited timeline for responsible entities to complete their assessments and mitigation efforts.

V. CONCLUSIONS AND ACTIONS REQUESTED

The Energy Policy Act of 2005 created a statutory impediment on federal regulators seeking to enact higher standards of security on responsible entities operating within the BPS. We are concerned that the regulatory framework may lead to delays in the implementation of security standards that would better protect the BPS infrastructure and the critical infrastructures that depend on its operation. We endorse the FERC's interpretation of the Section 215 provision requiring "due weight" to be given to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard without complete deference.[17] We believe that the FERC staff's technical expertise in control systems and cyber security and the proposals that they set forward in this rulemaking provide a valuable security perspective for the responsible entities charged with implementing these regulations.

A painful lesson from the September 11th attacks on our country is that a system is only as strong as its weakest link. On that day, several terrorists entered the U.S. transportation system through a small airport in Portland, Maine. Once inside the system, they were able to carry out their plans unimpeded. The Federal government must remain vigilant in eliminating weak links that can be exploited by those who wish to do us harm. In that vein, because of the interconnections between publicly- and privately-owned infrastructures that comprise the BPS, we believe that every responsible entity should be held to the same standards for securing their critical assets.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency non- national security operations and assets. In 2005, NIST released Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems." This publication was originally developed for use with traditional information technology systems. Recently, however, NIST established the Industrial Control System Security Project to improve the security of publicly- and privately-owned industrial control systems. The major focus of the

[17] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, Section 215(d)(5) (2005).

project is to clarify and rectify problems experienced in applying SP 800-53 to industrial control systems and develop new requirements in those areas. In December 2006, NIST published SP 800-53 Revision-1 that provides interim guidance on the application of the security controls to industrial control systems. These specifications are binding on federal government agencies.

NIST research also focused on comparing the proposed NERC Reliability Standards for cybersecurity with SP 800-53. According to a NIST-sponsored review published in March 2007, an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the NERC Reliability Standards, though the converse may not be true. For instance, in the Tempe outage and SQL Slammer Worm incidents, the NERC Reliability Standards allow for the exclusions of telecommunications and distribution equipment from the "critical assets" list. Under the SP 800-53 requirements, however, there is no similar exclusion, and it is reasonable to conclude that a responsible entity could identify and mitigate vulnerabilities in these assets prior to an incident. The technical report concluded that the NERC Reliability Standards are both "inadequate for protecting critical national infrastructure," and "inadequate for all electric energy systems when the impact of regional and national power outages is considered."[18] In its February 2007 comments on the FERC Preliminary Staff Assessment, NIST researchers concurred, stating that the NERC standards "do not provide levels of protection commensurate with the mandatory minimum federal standards (FIPS) prescribed by NIST."[19]

Because of the interconnectivity between Federally- and privately-owned elements of the BPS, inconsistent regulatory structures create weak links and potential vulnerabilities in the entire system. A responsible entity in the private sector may fully implement the NERC Reliability Standards but will fall short of the security measures implemented by a public entity. According to a report by MITRE sponsored by NIST, "to date, there has been no serious effort to ensure that the cyber security standards and best practices emerging from the electric power industry are consistent with the federal standards and guidelines being developed by NIST in response to the FISMA."[20] We believe that this is a significant problem that must be addressed immediately. Though the NOPR specifically declines to propose that NERC incorporate any provisions of the NIST guidelines in the CIP Reliability Standards, in light of the security concerns at issue in this rulemaking, we urge the FERC to modify the standard so that it incorporates aspects of SP 800-53 and the related NIST standards.

In closing, we applaud FERC for proposing these regulations. We are hopeful that both FERC and NERC will find these comments helpful and incorporate them when finalizing their

[18] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

[19] Stuart Katzke and Keith Stouffer, *Comments on the FERC Staff Preliminary Assessment of the NERC Proposed Mandatory Reliability Standards on Critical Infrastructure Protection issued* December 11, 2006 Docket RM06-22-000, Feb. 6, 2007.

[20] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

rules for cyber security.

10