NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Meeting Summary
# Cyber Security Order 706 SDT — Project 2008–06

**February 2, 2008 | 1–5 p.m. MST**
**February 3, 2008 | 8 a.m.–5 p.m. MST**
**February 4, 2008 | 1–5 p.m. MST**

**Adopted Unanimously February 19, 2009**

**Robert Jones and Stuart Langton, Facilitation and Meeting Design**

**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
## Sixth Meeting Summary,
## February 2–4, 2009
## Phoenix, AZ

**Meeting Summary Contents**

***Appendices***

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Cyber Security Order 706 Standard Drafting Team
# Sixth Meeting Summary,
# February 2–4, 2009
# Phoenix, AZ

## EXECUTIVE SUMMARY

The Chair and Vice Chair welcomed the members and welcomed Rob Antonishen, Ontario Power Generation as the team's newest member. NERC staff David Taylor conducted a roll call of members and participants in the room and on the conference call. They then reviewed with the team and participants the proposed meeting agenda. David Taylor reviewed with the team the need to comply with NERC's Antitrust Guidelines**.** The facilitators reviewed with the team the consensus guidelines adopted at the SDT November 2008 Little Rock meeting.

Scott Mix, NERC staff provided the team with an update on the status of the Technical Feasibility Exception white paper and the effort to convert it into a compliance document under NERC Rules of Procedure. On Wednesday, Scott Mix provided an additional update on the TFE process noting he had received an e–mail from the NERC Assistant General Counsel that outside counsel started to review the white paper and that nothing had been identified as a show stopper e.g. "good faith efforts".

In introducing the Phase II presentations and discussions, the facilitator reviewed related FERC 706 provisions noting they direct the SDT to consider "applicable features" of the NIST framework (Paragraph 25, 232, 233).

Bill Winters presented his paper, "Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection," and an additional section, "Thoughts for Discussion of NIST/CIP Opportunities" noting his assignment was to review the NIST/FISMA framework and suggest CIP features that represented strengths that might be incorporated into NIST/FISMA. His approach was to ask and try to answer the question: could my company apply the NIST/FISMA security framework approach? He suggested two approaches going forward: Heavy alignment vs. Integration Light:

1. *Heavy alignment* — replace/expand CIP 002 require assessment of: systems used in control and monitoring BES/BPS; systems directly connected and/or exchange data with; and systems which transport data used in control and monitoring.
2. *Light alignment* — develop a set of controls using NIST controls as starting points.

Members discussed topics that included: Address gaps in both NIST and CIP; Common Controls and Auditing; Outcomes Based Framework; Other Approaches; How prescriptive should controls be; Standards vs. Frameworks; and Certification Methodology.

John Lim presented the team's paper on Phase II approach from a CIP perspective on behalf of Jackie Collett, Scott Rosenberger and John Varnell. He noted that CIP standards are intended to be a baseline for cyber security for bulk power assets with a focus on assets with the highest impact. One of the issues with the current NERC standards which the team discussed the most was the "all or nothing" approach of the current CIP standards, i.e. if an asset is not defined as "critical" under CIP, there are no controls required. Perhaps additional systems and/or functions need to be identified to address this gap.

The team identified the following five issues with CIP 002 and for each offered comments on shortcomings, gaps, challenges and options: Piecemeal Approach; Not protecting assets needing protection; Gaming; All or Nothing Approach; and Loss of Asset Integrity and Misuse. John Lim noted that a multi–level protection scheme will have to identify high, medium and low. It will be necessary to study which assets are most critical. Look at the function of system and the connection to the BES.

Following the presentation there was a discussion about whether vulnerabilities in common systems should be addressed in the next version of standards. There was also discussion concerning the protection of defined Critical Assets versus protection of all SCADA systems. Several members stated that priority should be given to CIP 002 and the all or nothing view of defining Critical Infrastructure which is in scope as a result of CIP 002 current logic. Several members expressed that at least a minimum level of protection must be prescribed for additional assets.

Scott Mix took on the task of trying to conceptualize what would a NERC FISMA process look like to apply while maintaining the status quo in terms of the scope of the current CIP standards. He created a "straw man" which was presented in a power point format. He noted that he started with a mission focus on the bulk electric system (BES) vs. the bulk power system (BPS). The law and FERC say BPS whereas NERC has historically used the BES. He then noted that extending the scope into the distribution system will take an act of Congress because the bulk power system does not include distribution. The bulk power system consists of the 8 regional bulk electric systems. Characteristics are identified for 3 categories: confidentiality; integrity and availability. Then a high water mark is applied to the highest ranking of the 3 aspects. The electric system is bisected into Transmission and Distribution. Distribution is off the table by law. The portion of Transmission dealing with Marketing is also off the table. Transmission is then divided into High, Medium and low impact to the BES. If we applied that methodology to the standards this would classify all transmission assets by impact (high, medium, low, none). Then the SDT could go through CIP-003 through CIP-009 and determine what the implications are from a reliability standpoint. 800–53 is a good catalog that can be used for an approach excluding the sections that deal with financial, etc, which are not applicable. There are significant implications for the workload for SDT, the workload for education, and the workload for industry implementation. Scott suggested the SDT could have a healthy debate as to whether or not this approach is what the Team agrees is the right approach.

SDT member Michael Winter drafted these overarching principles for consideration by the SDT based on the team's previous review and discussion. He introduced them making the following points: these principles are intended to be complementary and not mutually exclusive; the SDT should modify in order get the best of both worlds; CIP and NIST. The concept is to offer protection for all but to different degrees based on the risk.

The top 3 most acceptable principles based on the SDT's initial ranking are:

1. Create clear standards and employ a technical exception/compensating controls reporting and guidance process that accommodates deviations (3.6 of 4)
2. A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any. (3.6 of 4)
3. Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact.

The following draft principles are in order of acceptability:

4. An entity's Asset classification would be open to scrutiny by regional entities and ERO. The extent of scrutiny to be defined and tightly controlled. (3.1 of 4)
5. Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP controls for each level. Address any gaps at the same time but keep the same CIP-002 to CIP-0XX general format. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it. (3.0 of 4)
6. Any IT devices beyond the perimeter, including telecom, are not part of the CIPs — the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted. (2.9 of 4)
7. As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high, moderate, or low classification of the physical perimeter, facility, or site within which it resides. Apply security controls based on the classification. (2,8 of 4)
8. Protect all cyber assets related to power system; not just the Critical Cyber Assets but to different degrees of protection/controls depending on their classification. (2.8 of 4)

The facilitators noted that the authors of the draft papers and principles would be asked to refine them and be prepared to present them at the February 18–19 SDT meeting.

For the Phase I review, the SDT reviewed all of the responses drafted to date for consistency and content. The team also looked at each of the additional industry comments that were not available at the January 7–9, 2009 Phoenix meeting. They then broke into the small groups that had been formed and worked together at the January meeting to complete the task of refining the responses. The SDT then reconvened and reviewed and agreed on the final responses.

On Wednesday, the SDT reviewed all of the proposed changes to the Phase I documents posted for industry review in light of the SDT responses and discussion. The SDT unanimously agreed to:

- Adopt the SDT Response Document (reflecting Tuesday's agreed on changes)
- Adopt the Proposed Changes to the Phase I Documents (reflecting Wednesday's review)
- Agree to post the documents for the 30–day pre-ballot period.
- However, the Phase I balloting will only commence after the NERC TFE proposal has been posted for industry comment for at least 14 days.

The SDT reviewed a draft set of Violation Severity Levels for the current CIP 003 through CIP-009 that a separate team (Project 2008–14) has developed. The SDT members expressed concerns with the likely confusion with the VSL team and in the industry posting both of these VSL changes (i.e. current CIP and Phase I proposed changes). Mr. Taylor noted that the draft SAR that directed the VSL SDT to only review the current CIP standard was open for comment until February 10, 2009. Members again expressed concerns that two SDTs revising the same documents is sure to cause confusion in the industry. Following straw polls, (the SDT to take on drafting VSLs for current CIP, Phase I, and Phase II standards 0–18; for the SDT to take on VSLs for Phase I and II, 7–11 in support; and for SDT addressing only Phase 2 VSLs, 16–2 in support, the SDT adopted the following approach:

The following statement will be forwarded to the SAR Committee as an SDT comment for its consideration with only the names of those SDT members voting in support of the motion:

> "The Phase I changes ("Version 2") to the CIP standards are expected to be balloted coincident with the development of the VSLs for "Version 1" of the CIP standards. The Project 2008–06 drafting team will not be in a position to include the VSLs with the revised standards due to the timing of the two projects. The VSL drafting team is best positioned to recommend VSLs in support of the Version 2 standards."

The motion was approved by more than 75 percent of the SDT members present and voting. The facilitators reviewed adjustments to the schedule including:

- A SDT comment on the VSL SAR by the deadline (February 10, 2009)
- February 18–19 in Fairfax, Virginia — advance the Phase II review and discussion
- March 10–12 in Orlando, Florida — seek a Phase II framework going forward.
- April 14–16 in Charlotte, NC — test the Phase II framework in a workshop with cyber experts and refine the framework for presentation at the MRC on May 1.
- May 1 — Members Representative Committee presentation of Phase II framework
- May 18–19 — Refinement to Phase II framework based on MRC comments and determination of whether to issue a white paper for industry comment. Review proposed SDT sub–committee and drafting group structure
- June–December, 2009 — SDT meetings along with SDT drafting groups.

The team then evaluated the meeting in terms of what worked and what could be improved. The meeting adjourned at 11:30 a.m.

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

## Cyber Security Order 706 Standard Drafting Team

### Sixth Meeting Summary,
### February 2–4, 2009
### Phoenix, AZ

## I. INTRODUCTIONS, AGENDA REVIEW, PROCEDURES AND OPENING REMARKS

The Chair and Vice Chair welcomed the members and welcomed Rob Antonishen, Ontario Power Generation as the team's newest member. NERC staff David Taylor conducted a roll call of members and participants in the room and on the conference call *(See appendix #2*). They then reviewed with the team and participants the proposed meeting agenda *(See appendix #1*).

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

The facilitators reviewed with the team the consensus guidelines (Appendix #5) adopted at the SDT November, 2008 Little Rock meeting.

## II. TECHNICAL FEASIBILITY EXCEPTION UPDATE

Scott Mix, NERC staff provided the team with an update on the status of the Technical Feasibility Exception white paper and the effort to convert it into a compliance document under NERC Rules of Procedure. He offered the following points:

- NERC's outside legal counsel is reviewing and helping to convert the whitepaper into a formal compliance document under NERC Rules of Procedure.
- The SDT needs to take into account all of the FERC rules regarding the NERC Rules of Procedure.
- Expect to see a short formal version in the ROP (400 series) and an appendix with greater detail.
- Being prioritized with all other filings. Unlikely to hear more by Wednesday, February 4, 2009. There is a large compliance filing in queue ahead of this tasking and we do not know if other work is ahead of the TFE document.
- Once the proposed procedure is ready, it will have a 45–day posting period for industry comments. Similarity to standards review, comment, and vote process is not yet clear. It must be adopted by the NERC BOT.
- NERC and the SDT understand that the Industry needs something now. Need to be able to process TFE by the end of the second quarter of 2009.

- Need to circle around on Wednesday to see if there is more information for the SDT prior to its approval to post the Phase I revisions for review and balloting.
- Dave Taylor noted that in Sacramento the SDT decided TFE was a separate process from Phase 1. He noted the Rules of Procedure process is likely to happen more quickly than the Phase 1 Standards process

**SDT Member Comments**

- TFE is a big gap that may impact the Phase 1 posting schedule.
- The schedule was to post the responses to comments and revisions to standards on February 5, 2009.
- The Standards Committee meets next week and would be expected to approve for pre–ballot posting.
- A lot of utilities will need to use TFE beginning July 1; they're asking members often what's going to be needed. As soon as possible, they need to know something for them to begin the process.
- Scott Mix added that he is not sure exactly what it will look like, but the SDT can assume the fields that appear in the white paper (standard referenced, etc.) that the SDT reviewed in December won't get stripped out. Some other entries may or may not be acceptable from a legal perspective. The key information that is likely to stay is the information that will take the longest time to develop.
- Entities are counting on the availability of technical feasibility.
- Once posted, can balloting be delayed?
- Are we going to let the clock drive us or are we going to do what is right?
- When will there be industry notice of what is happening?
- Large NERC and FERC compliance filing ahead of this.
- The industry has to be understanding of generation and substation devices. Implementing during the last half of this year.
- Industry needs to understand how this fits with standards development.
- Starts July 1 — need the TFE. Impact on response to industry of Phase 1 products?
- Need to get information, even if it is not in final form.
- Need process in place on July 1. Normally compliance processes take several months.
- If remove reasonable business judgment, must have TFE piece.
- We separated TFE from the standards and handled through compliance and rules of procedure. Industry hasn’t separated this in their understanding. Without clarity and certainty about how this is going to be handled, industry may reject phase 1 changes.
- The SDT is ready to help and also not advisable to post Phase 1 standards for balloting until something is out on the TFE process as well so the industry has what it needs.
- SDT shouldn’t authorize until TFE process is out in some form.

- The Chair and Vice Chair sent a memo to Mike Assante at NERC and copied Dave Cook, NERC General Counsel and Dave Taylor last week and he is aware of the SDT concerns about the importance of moving quickly so that the Phase 1 changes and the TFE process is known.
- Whenever it occurs, the industry wants to know what the TFE process will be and what it will need it by the end of the year. There may be a compliance issue and the industry needs to know how TFE fits into compliance, especially with CIP–007.
- If we get thru the comment response during this meeting, we may want to follow up on Wednesday.
- The Chair and Vice Chair suggested that perhaps a few of us can come up with an interim solution that we can review on Wednesday and will allow us to move forward.

On Wednesday, Scott Mix provided an update on the TFE process noting he had received an e-mail from the NERC Assistant General Counsel that outside counsel started to review the white paper and that nothing had been identified as a show stopper e.g. “good faith efforts”. In the SDT discussion the following points were made:

- One new point that they raised concerned “What can you claim a TF for?” Is it only what is called out in the standard, or is the subject broader that defined in the standard?
- Scott cautioned that we will have to wait for the outside counsel to complete their review.
- The majority of comments on such rules of procedure typically come from legal and upper management. The good news is that the process seems to be proceeding more quickly. He expects approval around the middle of the first round of ballots on standard changes. It is possible that the ballot should be delayed in order to ensure the opportunity of review if the SDT believes it is warranted.

## III. SDT 706 PHASE II FRAMEWORK REVIEW AND DISCUSSION

### A. FERC 706 Order Provisions

The facilitator reviewed related FERC 706 provisions noting they direct the SDT to consider “applicable features” of the NIST framework that might be applied to the CIP:

- “…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.” *FERC Order 706, Paragraph 25*

- "…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." *FERC Order 706, Paragraph 232*
- "…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." *FERC Order 706, Paragraph 233*

**B. White Paper Presentation — NIST/FISMA and CIP, Bill Winters**

Bill presented his paper, "Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection," and an additional section, "Thoughts for Discussion of NIST/ CIP Opportunities" and noted his assignment was to review the NIST/FISMA framework and suggest CIP features that represented strengths that might be incorporated into NIST/FISMA. His approach was to ask and try to answer the question: could my company apply the NIST/FISMA security framework approach? Below are points he made in his presentation:

1. One of the CIP problems is that it is a one size fits all approach. It doesn't distinguish between different big and small facilities and their relative security risks. NIST/FISMA with its focus on life cycle methodology, risk assessment methodology and matching the "controls." It offers more in bringing the electric industry forward in information and system security knowledge and application.
2. "Controls" are most common set of information to provide to industry as a common basis for implementation and protection and 853 represent a "hell of a body of controls." 853A is an assessment process for those controls.
3. The NIST/FISMA approach offers a good educational potential as its series of documents could easily be put together for a curriculum that could be offered industry wide to teach and get everyone up to an equivalent level of understanding of the NIST/FISMA framework which provides capability.
4. The NIST/FISMA framework is not currently targeted towards our kind of control systems (CIP based). But the industry can bridge that gap to meet our needs. You may not have to use only the controls presented in 853 as these could be augmented.
5. All gaps in CIP are largely covered in NIST/FISMA regarding controls regarding any entity type. Even where technical feasibility is limited.
6. The closer and sooner we can get to NIST framework, the faster we will get to a common set of controls across various entities; a framework then that vendors, and industry, will produce an infrastructure grounded in a common set of expectations.

**SDT Member Comments**

- "Frequently asked questions" may answer some of the NIST questions. Did the FAQ with the standards make it on the NERC Web site yet? The Standards Committee asked for more information on that and its posting is pending the SCs review.
- Most SDT members indicated they have seen questions.
- What was Bill's "plan of attack" in his review and drafting? He indicated he started with 853, FIPS 199 and 200, looked at the FISMA site, with all other documents (about 12 in number). They are voluminous but practical for drafting team to use this process. Bill's second paper addresses this. Is the SDT doing it or is it guidance to industry to do it?
- 853 caveat for control systems — Appendix J. NIST published white paper on control systems speaking to general architecture. How much is 853 applicable to control systems?
- SDT would have to tailor controls to fit our systems. The largest gap in the NIST/FISMA is that they don't address reliability.
- Review the FISMA appendix that addresses how to tailor the controls.
- NIST Draft 2 of 82 goes to next step and addresses control systems. Similarity between process control systems and BES control systems.
- CIP standards may need to be broken apart into: commercial computing environment; different standards in generation plants, etc.
- A plus is that the NIST/FISMA framework is developed and already paid for with tax payer dollars. We can leverage that expertise and apply and tailor it to our industry.
- He thought he would find a disjointed set of documents but was surprised to see the logic and connection of the framework. The SDT could get behind or alongside NIST/FSMA to further documents for the BES.

**Thoughts for Discussion of CIP/NIST Opportunities**

Bill Winters offered the following thoughts for the CIP/NIST/FISMA SDT discussion that were contained in a second paper he handed out to members:

1. He noted there are some controls in CIP but they are not related together.
2. A possible transition approach could be to walk through CIP standards and tie to NIST guidelines (e.g. analyze system, risk assessment process, etc). The SDT could do this relatively easily. The question would be how much detail we should go to.
3. The SDT could put together controls and break into small working groups to align controls to CIP standards.
4. SDT might recommend letting federal agencies subject to FISMA be able to use it to satisfy CIP requirements.
5. It may be better to create separate set of documents that serve as parallels for control systems vs. creating appendices for things like control systems.

6. Offers two approaches going forward: Heavy alignment vs. Integration Light.
7. *Heavy alignment* — replace/expand CIP-002 requires assessment of: systems used in control and monitoring BES/BPS; systems directly connected and/or exchange data with; and systems which transport data used in control and monitoring.
8. *Light alignment* — develop a set of controls using NIST controls as starting points.
9. Common controls would serve as the basis for certification. How proscriptive they are written will be debated.
10. The industry should be trying to get to a common set of protections and the controls are the fastest route there. Hard work up front, but down the road, there will be less work under a new NIST/FISMA system.
11. The NIST/FISMA framework will enable a more open discussion across the industry of the controls unlike today's CIP discussion.
12. Options in developing and implementing/phasing in over time: e.g. on vendor–by–vendor, system by system etc.

**Member Comments**

- **Address gaps in both NIST and CIP.** There are gaps for control systems that still need to be addressed in NIST. CIP has benefits for addressing these gaps.
- NIST needs an overarching document that provides step by step. "A read me first" document with an FAQ. There is a 36 pp Guide to NIST information security docs that serves as a roadmap for all docs on the NIST/FISMA website.
- Replace all CIP standards with one requirement? Implement a NIST based protection program to protect critical cyber assets. Would that be close to what the current CIPs provide? May not be close at all. Moving NIST into CIP — care has to be taken; we may end up with more holes
- Moving to be more strongly associated with NIST/FISMA might be better than sticking with where we are with CIP.
- Nothing precludes you from using NIST as basis for building standards. There is a small percent within the industry have to use NIST. A much larger percent can use CIP standards and come up with their own methodology and document in procedures how to do that.
- **Common Controls and Auditing.** You can do it however if you want to in CIP; some struggle with this. When it comes to auditing, what is the outcome? Most prevalent feature in NIST is that you can audit across the entities through the existence of common controls.
- How much reworking would be required to convert to a NIST/FISMA compliant program? There are many ways to meet requirements.
- The SDT's work and output will be roundly criticized if we adopt a narrow scope and basically leave the CIP as is it is now.
- **Outcomes Based Framework.** The SDT should remember the challenge Mr. Assante made to seek to develop an "outcomes based approach and standards". Standards that are

more prescriptive are presumably easier for auditors, but harder for industry to protect assets.

- Let the industry use tools out there as long as the end goal of protecting critical infrastructure is achieved. We are caught between multiple masters. NERC Compliance wants black and white standards requirements audited with a Yes or No.
- **Other Approaches?** In DC all we heard was NIST/FISMA. Are there other standards? Look across all to determine how to build guidelines to have protection. What would be entry to these? 199 document. E.g. all cyber assets in CIP-002 fit in high category. How we categorize systems?
- What would an outcome based standard look like? A "senior manager" outcome entity will put into place a governance program to ensure that an appropriate program is in place to maintain a good security program. Why should CIP mandate a single senior manager. Will FERC buy off? Outcomes may be hard to measure.
- Guideline about the types of people and roles for good practice. Let them figure out who will do. Somebody is responsible for all (1 or 10 different).
- SDT should be trying to move people in direction of NIST framework over the long term. This is "a" methodology.
- **How prescriptive should controls be?** What is the body of controls? Should we be prescriptive and identify a minimum set of protections for each type of system? CIP-002 through CIP-009 does it here and there but leaves a lot for interpretation.
- Trying to be as non–prescriptive in order to preserve choices in implementing security as long as certain goals are met.
- Standards should be telling you "what" to do not "how" to do. CIP may have stepped over the line on the "how" end. In order to make it auditable we may be forced to cross the line again with the "how". 199 and 200 are the standards and 853 a guide.
- If we put anything in a standard it becomes mandatory and enforceable; specifically if we put controls as to what we tell industry they must be doing. E.g. look at kinds of industry comments on the proposal to find a single person who will have to take responsibility. This will be nothing compared to 200–400 pp we will receive on this path.
- **Standards vs. Frameworks.** We need to be clear of difference between standards vs. framework. NIST is a framework that was not intended nor designed to be standards to be certified.
- **Certification Methodology.** We should focus on a framework and then what is the certification methodology we will use. How do we get to that so we are able to have a consistent set of protections?
- Current CIP based on 1200, which was based on ISO 17799. The SDT should pick a framework and develop the adaptation as they can all work. Then consistently implement that framework. All frameworks have provisions for certification.
- Should the SDT propose continuing down the ISO 17799 path? Or go to some other framework?

### C. Phase II — CIP and NIST/FISMA — CIP–002–1 Discussion Document, 1–29–09

John Lim presented the team's paper on behalf of Jackie Collett, Scott Rosenberger and John Varnell. He presented a discussion paper for the Phase 2 approach. He noted that the CIP standards are intended to be a baseline for cyber security for bulk power assets with a focus on assets with the highest impact. One of the issues with the current NERC standards which the team discussed the most was the "all or nothing" approach of the current CIP standards, i.e. if an asset is not defined as "critical" under CIP, there are no controls required. Perhaps additional systems and/or functions need to be identified to address this gap.

The team identified the following five issues with CIP-002 and for each offered comments on shortcomings, gaps, challenges and options:

1. Piecemeal Approach.
2. Not protecting assets needing protection. Description, comments, and options.
3. Gaming
4. All or Nothing
5. Loss of Asset Integrity and Misuse

John Lim noted that a multi–level protection scheme will have to identify high, medium, and low. It will be necessary to study which assets are most critical. Look at the function of system and the connection to the BES.

Following the presentation there was a discussion about whether vulnerabilities in common systems should be addressed in the next version of standards. There was also discussion concerning the protection of defined Critical Assets versus protection of all SCADA systems. Several members stated that priority should be given to CIP-002 and the all or nothing view of defining Critical Infrastructure which is in scope as a result of CIP-002 current logic. Several members expressed that at least a minimum level of protection must be prescribed for additional assets.

**Member Discussion Points**

- All or nothing. Definition of a cyber asset. "Something that is programmable." It is in the NERC glossary. What about network connectivity? Formal definition from NERC. How is programmable being defined?
- What about analogue?
- Programmable or programmed?
- Include anything with firmware. What about subclasses in security environment. Very few of those are left.

- **Focus on High Impact Assets.** Commonality of vulnerabilities — perhaps looking at functionality will address issue. Will focusing on high impact assets address common vulnerability?
- Should this be addressed in standards or in the vulnerability assessment and response system? E.g. “Zero day exploits” problem — the risk of acts that take systems down before we realize vulnerability. Apply good basic security standards and you can deal with this. But if we only look at high impact systems, we may not be addressing this.
- **System Approach.** Industry can/may use a system approach. However, won’t do this voluntary. Whatever is not critical asset. This approach doesn‘t conform with information security. Can we redefine some of these things in standards? No just programmable devices. CIP standards may not be sufficient.
- Many in industry are protecting others even though standard doesn’t require. Put critical asset in because that is what they are going to get fined for. You can keep off the CA books but still protect.
- Already addressed/protected in CIP-005
- If this involved anything except critical infrastructure I would trust that people will do the right thing. Don’t call cyber security call them reliability.
- System perspective approach — today people only admit to 30 percent of what they have. However, FERC’s jurisdiction to BES is tied to interstate commerce moving of power. Bulk power assets is a limited portion of what falls under FERC’s jurisdiction. Critical asset list. N– 1, 2, 3 and extreme contingencies. Cyber event — could be in an N–4, 5, 6. From a system perspective, this increases which assets are ‘critical”
- Dump CIP-002 and start over again?
- From a NERC standpoint we need to focus on potential attack vectors and will increase in the future.
- Have to study the criticality of the systems we are doing.
- Look at NERC charter — BES doesn’t cover every device — agree, but we need to be looking far enough forward to be able to protect that. The end goal is to protect BES, but extent to which the distribution affects BES, we need to be considering whether or not distribution can impact BES and if so, what to do at that level what needs to happen.

### D. Strawman — NERC/FISMA Asset Selection Process — Scott Mix

Scott Mix took on the task of trying to conceptualize what would a NERC/FISMA process look like to apply while maintaining the status quo in terms of the scope of the current CIP standards. He created a “strawman” which was presented in a PowerPoint format. He noted that he started with a mission focus on the bulk electric system (BES) vs. the bulk power system (BPS). The law and FERC say BPS whereas NERC has historically used the BES. He noted that some standards have drawn line at various levels and the CIP standards focus only on high impact systems. Most of NIST framework deals with technical protections once assets have been identified.

Scott noted that the FISMA approach requires that all computer assets be included in scope. Using FIPS–199, systems are in scope if needed to accomplish the assigned mission.

He then noted that extending the scope into the distribution system will actually take an act of Congress because the bulk power system does not include distribution. The bulk power system consists of the eight regional bulk electric systems. Characteristics are identified for 3 categories: confidentiality; integrity and availability. Then a high water mark is applied to the highest ranking of the 3 aspects.

Electric system is bisected into Transmission and Distribution. Distribution is off the table by law.

The portion of Transmission dealing with Marketing is also off the table. Transmission is then divided into High, Medium, and Low impact to the BES. Perhaps there needs to be a fourth category that is "ignore" or no impact to reliability. If we applied that methodology to the standards this would classify all transmission assets by impact (high, medium, low, or none). Then the SDT could go through CIP-003 through CIP-009 and determine what the implications are from a reliability standpoint. 800–53 is a good catalog that can be used for an approach excluding the sections that deal with financial, etc, which are not applicable. A key question is would this meet all mandated changes for FERC 706? There are significant implications for the workload for SDT, the workload for education, and the workload for industry implementation. Scott suggested the SDT could have a healthy debate as to whether or not this approach is what the team agrees is the right approach.

**SDT Member discussion**

- Mainly affect CIP 5, 6 7? Yes but also others.

### E. Overarching Principles Presentation and Review — Mike Winters

SDT member Michael Winters drafted these principles for consideration by the SDT. He introduced them making the following points:

- Hoping principles are complementary
- Modify existing standards and get the best of both worlds– CIP and NIST.
- Risk of scrapping and starting over.
- Consider the amount of IT introduced to distribution systems.
- These principles are not mutually exclusive.
- #1, 3 and 5 are consistent with Scott Mix's strawman.
- The concept is to offer protection for all cyber assets associated to operating the interconnected power system but to different degrees based on the risk.

**SDT Member Comments before Ranking**

- Why not use guideline by Risk Development Working Group?
- Pick a framework. Apply it consistently. 800–53 catalogue – 003–009.
- All cyber assets “Power system”. There is not a nice line around generation systems. [Note to Draft: Generation is a critical component to power systems]
- The term Power System IT is simply intended to differentiate from corporate IT.
- Potential for causing someone to make a decision to shut down a plant?
- E.g. continuous emissions monitoring. Fuel supply and multiple infrastructure interdependencies. This is a big issue. SDT can’t get to this point for a long time.
- Approach for #1 — catalogue your SCADA, (EMS systems, etc.) and then look at those systems essential to operation of inner circle.
- What is the list of critical assets minimum to perform our mission? Why protect anything else? Or the reverse — identify which assets are critical in order to meet mission. Determine which assets, if turned off, would prove to be critical to meet mission.

## Phase II Overarching Principles (Michael Winters)
## February 2 SDT Initial Rankings

**The Overarching Principles have been re–ordered to reflect the ranking of each principle and their average acceptability from higher to lower. The Strikethrough #s reflect the initial numbering.**

1. **(2) Create clear standards and employ a technical exception and compensating controls reporting and guidance process that accommodates deviations.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **11** (10/1) | **5** | **1** | **0** | **3.6 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #2 outcome based, not too prescriptive — Exception based standards. Need a clear process with clear standards and TFE process and guidance to accommodate deviations.

2. **(8) A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **11**(10/1) | **2** | **2** | **0** | **3.6 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #8 Mapping — refers to NIST 800–53 Appendix G.

3. **(3)Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **9 (**8/1 ph) | **6** | **2** | **0** | **3.4 of 4** |

*Author's clarifying comments before SDT initial ranking*

- Principle #3 strike/delete from principle reference to going below 100kV. This should be considered "evolution" vs. "revolution."

4. **(4)An entity's Asset classification would be open to scrutiny by regional entities and ERO. The extent of scrutiny to be defined and tightly controlled.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **4** (3/1) | **11** | **2** | **0** | **3.1 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #4 allows for scrutiny — "open up the kimono" and have peer reviews or have asset classifications scrutinized by RRO and ERO. Will need and effective arbitration/mediation mechanism.

5. **(7)Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP controls for each level. Address any gaps at the same time but keep the same CIP002 to CIP0XX general format. Industry knows this format, is building policies and programs around it, has commented on it and has voted on it.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **5** (4/1) | **8** | **4** | **0** | **3.0 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #7 Use guideline to figure out the controls at different levels. Some customization, reference NIST, Use as starting point.

6. **(6) Any IT devices beyond the perimeter, including telecom, are not part of the CIPs – the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **4** (3/1) | **6** | **6** | **0** | **2.9 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #6 — logistics — interfacing devices and perimeters. Keep perimeter based or trusted zones, still accomplish.

7. **(5) As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high/moderate/low classification of the physical**

**perimeter/facility/site within which it resides. Apply security controls based on the classification.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **4** (3/1) | **6** | **7** | **0** | **2.8 of 4** |

*Author's clarifying comments before SDT initial ranking*

- #5. This is logistical and is related to principles #1 (8) and #3 (3)

**8. (1)Protect all cyber assets related to power system – not just the Critical Cyber Assets – but to different degrees of protection/controls depending on their classification.**

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | **3** (2/1) | **8** | **6** | **0** | **2.8 of 4** |

The facilitators noted that the authors of the draft papers and principles would be asked to refine them and be prepared to present them at the February 18–19 SDT meeting. That meeting would be devoted to making progress on the SDT's development of a Phase II framework around which the team could organize its work and begin more detailed review of the CIP and the applicability of the NIST.

## IV. PHASE I INDUSTRY COMMENT/ SDT RESPONSES

The Chair proposed that the SDT review all of the responses and then, as needed, break into the small groups that had been formed and worked together at the January meeting to complete the task of drafting the responses. The SDT then would reconvene and review and agree on the final response. Following that the SDT would review any changes made in the Phase 1 documents that were out for comment based on the SDT's responses.

Joe Bucciero presented the draft Response Text noting where there were additional responses needed. (See, Appendix #4 for link to a power point presentation). The team looked at each of the additional industry comments that were not available at the January 7–9, 2009 Phoenix meeting. The SDT reviewed and made suggestions related to consistency and content for the small working groups to consider keeping in mind the goal of "good enough to post" the responses. The six small working groups were re-formed to review the industry comments and to refine the SDT's responses. The six groups were created to craft the SDT's responses and to make appropriate edits to the text of the CIP standards.

The small groups reported the results of their drafting later in the afternoon to the full SDT which approved them pending the development of the complete text that was to be developed overnight by Joe Bucciero along with a redline draft of  the Phase I documents with changes made as a result of the industry comments.

On Wednesday, the SDT reviewed all of the proposed changes to the Phase I documents posted for industry review in light of the SDT responses and discussion.  The final SDT response document reflecting all of the changes agreed to by the SDT on Tuesday was not ready in final form for the team's review.  The Chair asked Mr. Bucciero to distribute the final Response document to the SDT as soon as it was ready.

Kevin Perry made a motion which was seconded by Tom Hofstedder that the SDT will:

- Adopt the SDT Response Document (reflecting Tuesday's agreed on changes)
- Adopt the Proposed Changes to the Phase I Documents (reflecting Wednesday's review)
- Agree to post the documents for the 30 day pre-ballot period.
- However, the Phase I balloting will only commence after the NERC TFE proposal has been posted for industry comment for at least 14 days.

The motion was unanimously adopted by all SDT members present and voting.

## V. VSL PROCESS AND DISCUSSION

Dave Taylor, NERC staff reminded SDT members that under the FERC Order 706 the Violation Severity Levels needed to be applied to the CIP 002 through CIP-009.  The Standards Committee made a decision to have a separate team assign VSLs to the standards rather than incorporating into the 706 SDT.  Project 2008–14 is creating the VSLs.  An initial draft of the VSLs is complete, but still needs to be posted for comment.  These draft VSLs will ultimately need to be compatible with CIP Phase I efforts of the SDT.

There were questions concerning the relationship of measures vs. VSLs.  Mr. Taylor reminded the group that the only thing which is required is the requirements and not the measures.

The SDT discussed the fact that a separate team created the VSL.  Mr. Taylor suggested that the original VSLs be posted and then revisions related to this SDT Phase I work could also be posted for comment.  The SDT members expressed concerns with the likely confusion with the VSL team and in the industry posting both of these VSL changes (i.e. current CIP and Phase I proposed changes).  Mr. Taylor noted that the draft SAR that directed the VSL SDT to only review the current CIP standards was open for comment until February 10, 2009.  Members again expressed concerns that two SDTs revising the same documents is sure to cause confusion in the industry. There was discussion regarding whose responsibility it is to create VSLs for the CIP original and Phase I revisions to CIP.  There was also discussion concerning the changes and timing or Phase I changes.

The facilitators suggested straw polling to determine the SDT's views on several options going forward.

- **Poll 1**: This team should take on both the CIP current VSLs (Version 1) and Phase 1 (Version 2) and Phase 2 (Version 3) CIP VSLs — **0–18 members supported** this approach.
- **Poll 2**: The VSL team should do both current CIP VSLs (Version 1) and the Phase I VSLs (Version 2) — **16–2 in support of this approach.**

Member Comments following Poll 2

- One member expressed concern about the amount of time it will take for this SDT to agree on comments to be sent on the other team's SAR. That member suggested that individual utilities should comment on the SAR, but consensus is not needed.
- **Poll 3:** The SDT should be responsible for VSL's for both Version 2 (Phase I) and Version 3 (Phase II) of VSL's — **7–11 in support** of proposal.

Following the polls and further discussion, a motion was made by Kevin Perry and seconded by Sharon Edwards as follows:

The following statement, if approved by the SDT, will be forwarded to the SAR Committee as an SDT comment for its consideration with only the names of those SDT members voting in support of the motion:

> **"The Phase I changes ("Version 2") to the CIP standards are expected to be balloted coincident with the development of the VSLs for "Version 1" of the CIP standards. The Project 2008–06 drafting team will not be in a position to include the VSLs with the revised standards due to the timing of the two projects. The VSL drafting team is best positioned to recommend VSLs in support of the Version 2 standards."**

The motion was approved by more than 75 percent of the SDT members present and voting.

The following SDT members voted in favor of sending the following SDT comment to the VSL SAR Committee with their names appended: Jeri Domingo Brewer; Kevin Perry; Jon Stanford; Rob Antonishen; Sharon Edwards; Jay Cribb; Joe Doetzl; Scott Fixmer; David Revill; Phil Huff; Tom Hofstetter; Chris Peters; Keith Stoffer; and Gerry Freeze

The following SDT members voted against the motion: Rich Kinas; John Lim; John Varnell; and Kevin Sherlin.

## VI. NEXT STEPS

The facilitators reviewed adjustments to the schedule including:

- A SDT comment on the VLS SAR by the deadline (February 10, 2009)
- February 18–19 in Fairfax, Virginia — advance the Phase II review and discussion
- March 10–12 in Orlando, Florida — seek a Phase II framework going forward.
- April 14–16 in Charlotte, NC — test the Phase II framework in a workshop with cyber experts and refine the framework for presentation at the MRC on May 1.
- May 1 — Members Representative Committee presentation of Phase II framework
- May 18–19 — Refinement to Phase II framework based on MRC comments and determination of whether to issue a white paper for industry comment. Review proposed SDT sub–committee/drafting group structure
- June–December, 2009 — SDT meetings along with SDT drafting groups.

The team then evaluated the meeting

- **What worked?**
    - Small group breakout
    - Papers for Monday’s presentation available for advanced review
    - Rapid parking lot

- **What could be improved?**
    - Meeting announcement/agenda versus actual schedule — try to clarify and establish starting and ending times so people can book appropriate travel.
    - 4–3–2–1 vote language needs to be a bit tighter and clearer. Need to allow sufficient time in the session to understand proposals that will be ranked.
    - Underestimation of level of effort to get updated documents available on the last day.
    - Hard to keep track of where we were in the comments list. Needed unique identifier for reference purposes when we do this again.

- **Suggestions for next meeting**
    - Earlier agenda posting (with caveat that there are only two weeks separating meeting on February 18–19).
    - Possible pre–meeting SDT agenda review for future meetings?
    - Consider ways to survey experts

The SDT adjourned at 11:30 a.m.

**Appendix # 1**

## Meeting Agenda — February 2–4, 2009

### Draft Meeting Objectives:

- To receive an update on the NERC Technical Feasibility Exception process;
- To complete and adopt the SDT's responses to comments and any changes to the Phase I documents for posting;
- To initiate a SDT review of Phase II principles and potential approaches to integrating CIP and NIST/FISMA; and
- To agree on next steps and the work plan going forward.

**Monday February 2, 2009**

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

- Roll Call
- NERC Antitrust Compliance Guidelines
- Facilitator Review of January meeting and adoption of January 7–9, 2009 Meeting Summary

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

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

- Overview of Phase I Work–plan, January– May 2009
- Overview of Phase II Work plan– January–June, 2009– including CIP 002 conceptual approach and workshop and industry input and feedback.

1:40 Update on Phase I SDT Responses to Comments and Procedure Going Forward for Day Two — Jeri Domingo–Brewer

1:50 Update on Technical Feasibility Exception (TFE) Process — Scott Mix

2:00 Introduction to Phase II Review Process — Stuart Langton

2:10 Initial Review of Phase II Principles — Michael Winters

3:00 Break

3:15 Initial Presentation and Discussion of the Phase II White Papers — John Lim (Jackie Collett, Scott Rosenberg, and John Varnell) Bill Winters

4:55 Summary of Day One Outcomes and Review of Day Two Agenda

5:00 Recess

**Tuesday February 3, 2009**

8:00 Welcome, Agenda Review and Review of Day One Results

| | |
|---|---|
| 8:05 | Review of Proposed Procedure/Guidelines for Phase I Comment Review |
| 8:10 | Phase I Comment Review and Refinement — Plenary Discussion of Comments |
| 10:15 | Phase I Comment Review and Refinement — Plenary Discussion of Comments |
| 12:00 | Working Lunch (Return to plenary meeting at 2:00)<br>Small Group Breakouts — Review and Draft Final Responses (As needed) |
| 2:00 | Small Group Reports on Draft Responses and Plenary SDT Discussion and Decisions |
| 3:30 | Break |
| 3:15 | Small Group Reports on Draft Responses and Full SDT Discussion and Decisions |
| 4:50 | Summary of Day Two Outcomes and Review of Day Three Agenda |
| 5:00 | Recess |

| **Wednesday** | **February 4, 2009** |
|---|---|
| 8:00 | Welcome and Agenda Review |
| 8:10 | Review and Adoption of Phase I Responses and Proposed Changes to Phase I Products |
| 10:00 | Review of Work plan for Phase I and Phase II |
| 10:30 | (If time permits) Continue Review and Discussion of the Phase II Approach to Integrating CIP and NIST/FISMA. |
| 11:15 | Next Steps on Phase II Approach Development |
| 11:30 | Technical Feasibility Exception Process Going Forward — Scott Mix |
| 11:45 | Meeting Evaluation — What Worked and What Could be Improved? |
| 11:55 | Assignments, Next Steps and Review of February and March SDT Agendas |
| 12:00 | Adjourn |
| 12:15 | Working Lunch and Opportunity for SDT Small Groups to Continue Development of Phase II Products |
| 3:00 | Conclude |

**Appendix # 2**

**Cyber Security for Order 706 SDT Attendees List**
Phoenix AZ
February 2–4, 2009

### Attending in Person — SDT Members

| | |
|---|---|
| 1.Rob Antonishen, | Ontario Power Generation |
| 2. **Jeri Domingo–Brewer, Chair** | U.S. Bureau of Reclamation |
| 3. Jay S. Cribb | Information Security Analyst, Principal, Southern Company Services, Inc. |
| 4. Joe Doetzl | Manager, Information Security, Kansas City Power & Light Co. |
| 5. Sharon Edwards | Project Manager, Duke Energy |
| 6. Tom Hoffstetter | Midwest ISO, Inc |
| 7. Scott Fixmer | Senior Security Analyst Exelon Corporate Security, Exelon Corp. |
| 8. Gerald S. Freese | Director, Enterprise Information Security America Electric Power |
| 9. Richard Kinas | Orlando Utilities Commission |
| 10. John Lim | CISSP, Department Manager, Consolidated Edison Co.NY |
| 11. **Kevin B. Perry, Vice Chair** | Director, IT–Infrastructure, Southwest Power Pool |
| 12. Christopher A. Peters | ICF International |
| 13. David S. Revill | Georgia Transmission Corporation |
| 14. Kevin Sherlin | Sacramento Municipal Utility District |
| 15. Keith Stouffer | National Institute of Standards & Technology |
| 16. John D. Varnell | Technology Director, Tenaska Power Services Co. |
| 17. William Winters | Hydro One Networks, Inc. *(Monday only)* |
| *1. Roger Lampilla* | *NERC* |
| *2. David Taylor* | *NERC* |
| *3. Scott R. Mix* | *NERC* |
| *4. Joe Bucciero* | *NERC/Bucciero Assoc.* |
| *7. Robert Jones* | *FSU/FCRC Consensus Center* |
| *8. Stuart Langton* | *FSU/FCRC Consensus Center* |

### SDT Members Attending via WebEx and Phone

| | |
|---|---|
| 18.Phillip Huff | Arkansas Electric Coop Corporation |
| 19.Jonathan Stanford | Bonneville Power Administration |
| 20.Michael Winters | Hydro One |

### SDT Members Unable to Attend

| | |
|---|---|
| 1. Jackie Collett | Manitoba Hydro |
| 2. David Norton | Policy Consultant, CIPEnergy Corporation |
| 3. Scott Rosenberger | Luminant Energy |
| 4. Bryan Singer | Kenexis Consulting Corp. |

**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 Phase I documents and the Draft SDT Response Document and PowerPoint presentations by Joe Bucciero (Phase I review), Scott Mix (Phase II Strawman) and David Taylor (Phase I VSLs) reviewed by the SDT during the small group and full team discussions in Phoenix, AZ:

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

**Appendix #5**

## Background, Principles, and White Paper and Strawman Documents

## 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.

### Phase II Overarching Principles (*Michael Winters)*

***NOTE**: The principles below were drafted and submitted by SDT member Michael Winters. He notes they are applicable to both the 'NIST approach' and the 'CIPs modification' approach and suggests that the approaches may be one and the same. He requests that SDT members "Don't get hung up on any specific term as this is a concept. Terms and definitions can be refined."*

***Note from Michael Winters**: The approach suggested uses an example of facilities/sites being Critical Assets. Consider this a case study where we could then make the 'CA=System' model also work. These principles represent a collection of ideas voiced by several members at previous SDT meetings. It focuses on building upon existing CIPs for improvement rather then starting at the beginning. The foundation for the principles consists of: existing CIPs; NIST 800–53/82; SDT discussion and debate to–date. We have all observed that the SDT has made a few different attempts at finding the starting point for the next phase of changes and the overarching principles to be applied to those changes. It may be time to attempt an approach and then assess its effectiveness at an interim checkpoint. Even if we end up abandoning a main concept, some of the learning's will prove useful for future iterations. Leveraging the existing CIPs instead of a wholesale re–write will still accomplish an incorporation of NIST 800–53/82 where applicable without losing all the good work that has already gone into the CIPs or it being perceived by Industry that their investments in becoming CIP compliant to–date will be stranded.*

**1.** Protect all cyber assets related to power system — not just the Critical Cyber Assets — but to different degrees of protection/controls depending on their classification.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | |

**2.** Resist creating exception–based standards to accommodate every possible business and operations scenario. Instead, create clear standards and employ a technical exception/compensating controls reporting and guidance process that accommodates deviations.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | |

**3.** Use a consistent risk–based model to classify all assets (i.e. facilities, sites, physical perimeters) (i.e. not cyber assets at this point) as critical/high impact, moderate impact, low impact. Risk Assessment Working Group may be providing a good start and perhaps concepts from FIPS 199 impact analysis can also be incorporated.  This will allow for expansion of standards beyond Critical and to Distribution networks (i.e. below 100 kV – accommodates AMI, Dx automation, etc).  Classifying at the physical perimeter level would allow different classifications to exist within a building or at a site (e.g.  control room, computer rooms, dev and testing rooms, and back–office at a control centre).

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | |

**4.** An entity's Asset classification would be open to scrutiny by regional entities and ERO.  The extent of scrutiny to be defined and tightly controlled.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | |

**5.** As part of a power system (non–corporate IT) inventory of cyber assets, add an attribute to each device that associates the high/moderate/low classification of the physical perimeter/facility/site within which it resides.  Apply security controls based on the classification.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | **of 4** |

**6.** Interfaces between ESPs/PSPs of two different classifications will take on the controls of the higher classification.  Any routers, switches, firewalls, secure FTP, ICCP, DMZ that connects corporate admin networks or external entities to your power system IT (cyber) devices/perimeters get included as a CIP protected device.  Any IT devices beyond the perimeter, including telecom, are not part of the CIPs – the CIPs remain perimeter–based where devices on and within the perimeter are protected and everything beyond is considered untrusted.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | **of 4** |

**7.** Use the minimum security controls for high, moderate, low within NIST 800–53 to help model the CIP controls for each level.  Address any gaps at the same time but keep the same CIP002 to CIP0XX general format.  Industry knows this format, is building policies and programs around it, has commented on it and has voted on it.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | **of 4** |

**8.** A mapping similar to NIST 800–53 Appendix G to CIPs will help quantify and assess the gap, if any.

| *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.* |
|---|---|---|---|---|---|
| **2–2–09 rank** | | | | | |

**DRAFT** **01/29/09**

## Independent assessment of FISMA and related NIST documents for adoption for Electric Sector Critical Infrastructure Protection.

*William Winters, Arizona Public Service*

*(Distributed before the Meeting)_*

### What

First, I have to commend the NIST staff responsible for the development of the guidelines and standards documents that form the FISMA framework. This body of work provides an incredibly comprehensive background and framework for information security.

To a limited degree, the current version of CIP standards at least attempted to capture the essence of fundamental cyber security implementation and management however, as is evidenced by the creation of the SDT, the full extent of what is required was missed. In the years since the CIP standards were conceived, NIST expanded and refined the cyber security framework and standards documents required for FISMA. These documents embody the essence and the detail required for Information Security Management. In fact, the NIST FISMA documents go beyond a framework by providing the narrative background at a fundamental level necessary to develop a clear understanding of the framework, intent and method of implementation to non–cyber security professionals. A clarity that is largely lacking in the CIP standards.

To date the SDT 706 Phase II discussions have largely centered on NIST 800–53 and integration with the CIP standards. To a lesser degree, FIPS–199, NIST 800–53A and FISMA have been discussed.

I feel at this time expanding the discussion to FISMA and the full body of associated NIST standards and guidelines is warranted. Not simply should or how NIST 800–53 can be integrated but to what degree should or can CIP integrate or parallel FISMA.

After review of FISMA as documented and the supporting NIST documents, I count myself an advocate of integration and, to a significant degree, adoption of the FISMA/NIST approach to Information Security Management for electric sector CIP standard.

### Why

The FISMA/NIST framework provides a consistent methodology to install a set of security protections appropriate to the criticality of an information system and the associated information.

It is well thought out, documented and based on the fundamentals of cyber security and SDLC. The guidelines provide the fundamental security background as well as the guidance for application.

It is a body of work that is easily accessible by all industries and sectors and all sizes of entities, service providers, vendors, auditors, etc. It is a requirement for federal agencies including those in the electric sector. As such, it represents a common framework. Ambiguity is minimized. Knowledge sharing is maximized.

The use of a common framework will provide the greatest opportunity for uniform application of cyber security controls to protect our Critical Infrastructure. Fundamentally, it provides a common basis for assessment, implementation and audit regardless of sector or service entity.

As much as the existing CIP standards may get most entities to the point of implementing appropriate cyber security controls, it will not have been done in a consistent manner with clear mutual understanding of the objectives.

Though the body of NIST documents is of significant volume, the effort required to understand and apply is in no way more difficult than the effort that has been expended to understand and apply the CIP standards. The most significant difference is that after the NIST process is assimilated, security controls may be implemented consistently, monitored consistently, changed consistently and, assessed consistently.

Protecting our cyber managed supply of electricity in a consistent manner across all entities is the best thing to do.

It’s paid for.

### How

Integration approaches can range from drawing on individual elements in the NIST documents to fill in the CIP gaps requirement by requirement to wholesale adoption of FISMA.

My recommendation is that we take an approach that establishes a strong parallel to FISMA, utilizing the NIST standards and guidelines as much as possible.

In its most pervasive manifestation, this would entail a combination of adopting the FISMA/NIST documents directly and/or creating parallel documents/supplements tailored to the electric sector. This would likely result in an overhaul of the current CIP requirement layout and require transition education.

At a minimum, this would entail developing a set of controls (800–53), related assessment procedures (800–53A) and FIPS 200 Minimum Security Requirements equivalent specific to BES entities, creation of FIPS 199 Security Categorization equivalent that integrates to CIP 002 and other CIP requirements to relevant NIST documents.

The degree to which the FISMA/NIST framework should be adopted will need to be discussed and debated.

A couple of fundamental questions:

- Does FERC feel that adoption of FISMA/NIST framework will meet all the concerns in Order 706?
- What were the concerns with adopting the FISMA/NIST framework as the basis for the existing CIP standards and do those concerns still exist?

**W Winters 02/02/09**

**Thoughts for discussion of CIP/NIST opportunities**

***(Handed out at the meeting)***

- Develop set of controls for each area/entity which could be done regionally
- Entities can create control extensions. This is currently allowed in the NIST method
- Allow option for federal entities currently subject to FISMA and CIP to use FISMA/NIST to satisfy CIP
- Encourage use of FISMA/NIST today. Entities have the option today to use FISMA/NIST as a basis for meeting CIP requirements.

- Develop a process for application of FISMA/NIST (e.g. Develop as an overlay of CIP or Develop as standalone )

**Controls Development Approach**

- SDT sub–team(s) could develop initial minimum controls (they could be entity tailored controls and/or “exception” based controls)
- Create clearinghouse for sharing of controls amongst entities as different organizations develop control extensions
- Develop controls using working group model at the regional level. This could be extended to development of educational framework and more effective open information sharing.
- Lifecycle management of controls for improvement/refinement and adoption
- Regional controls could feed to national and periodic update with regional, national and NIST representation.
- NIST and/or SDT team create initial draft of documents for “CIP” (e.g. appendices to existing or separate set of docs,)
- Build transition education program based on mapping of CIP to NIST.
- As body of controls are refined and standardized, auditors, developers of compliance programs (internal, consultant/vendor), developers of applications, support personnel, etc. have common reference and interpretation of the standards

**Heavy alignment:**

1. Expand/replace CIP 002 to require assessment of:

   a) Systems used in control and monitoring of BES/BPS
   b) Systems directly connected and/or exchange data with
   c) Systems which transport data used in control and monitoring

2. Develop equivalent FIPS 199, FIPS 200
3. Develop Risk Assessment process (800–37 equivalent/appendix) tailored to industry.

**Integration light (in the beginning):**

1. Develop set of controls (can use existing NIST controls as starting point) for each of the CIP requirements.  Some of these exist within the CIP standards today but not consistently.
2. Systems that are determined in CIP 002 to be CCA are classified as high, as are all systems within the same ESP and form the ESP.  Monitoring systems get medium?
3. 3Map CIP requirements to NIST docs as guidelines particularly for Risk Assessment

## CIP–002–1 Discussion Document, 1–29–09

*Jackie Collett, John Lim, Scott Rosenberger, and John Varnell*

### I. Original Intent of the CIP–002 Version 1 Standard

- **Starting Point**: A "reasonable" initial attempt to applying cyber security to the electric infrastructure.
  - Initial Baseline – starting from zero
- High Impact Focus: Reduces the scope of implementation to the transmission and generation assets which have the highest impact on the reliability and operability of the BES.
- Cyber Assets: directly linked to the BES elements *FAQ Q2*
- Cyber Asset Scope: limited to control centers, remote access and "jumping–off" points, which may not be evident in the standard *FAQ 2*
- What to Do: Not How to Do
- Non–prescriptive: Allows flexibility for a wide range of scenarios

- **Key Decisions**:
  - Create "trusted zones"
  - Exclude communications outside of "trusted zones": often external carriers and indeterminate paths

- **Assumptions**: Not explicit in the standard, but required for good security
  - **Redundancy**: Critical Asset / Cyber Asset redundancy does not eliminate the requirement for cyber protection. *FAQ Q5*
    - Need to protect common modes of failure.
    - Multiple attacks / compromises are possible electronically.
  - **"Systems approach"**: A systems approach to identifying Critical Assets / Critical Cyber Assets can and should be used. CIP–002 does not preclude a systems approach, but does not explicitly require it.
  - **"Consider"**: Consider means include if at all applicable.
  - **"Essential to operation":** Critical Assets and Critical Cyber Assets should be identified and protected to ensure sustainable and reliable operation indefinitely. Loss or compromise of the Control Centre or other critical functions is not sustainable.
  - **Critical Assets**: Critical Assets may include sites, elements and systems.
  - **CCA Compromise**: In addition to the BES impact due to loss of the Critical Asset or Critical Cyber Asset, compromise of the Critical Cyber Asset must be included in the risk assessment (Integrity).
- FERC conditionally approved the Version 1 standards, and directed changes for a "final" version

- The “gap” is what is currently under discussion

## II. Important Aspects of CIP–002–1

1. **Relationship to BES**: There is a very clear relationship between the BES assets required for reliability and the cyber assets essential for their operation.  The reliability and operations segments of the electric industry are structured upon BES assets.  This includes processes, procedures, inventories and terminology.
2. **High Impact Focus**: CIP–002–1 focuses the efforts and resources for protection to the most important BES assets and associated cyber assets, recognizing that resources are not unlimited.  Assets which do not affect the reliability and operability of the BES are not considered.  As a result, the majority of the BES assets are not included for protection under the CIP standards.
3. **Industry Acceptance**: The electric industry has invested thousands of hours and millions of dollars to meet CIP–003–1 through CIP–009–1 based on CIP–002–1.  The industry would not favor a significant or radical change to the asset identification method, and could reject it.

## III. Issues identified with the current CIP–002 + Standards

| | |
|---|---|
| **A** | **Piecemeal Approach** |
| ***Description*** | By identifying individual Critical Cyber Assets, security gaps exist when the CCAs operate in a system.  (E.g.  data integrity impact for a cyber asset outside of the ESP) |
| ***Comment*** | • The identification of Critical Cyber Assets does not preclude a systems approach, but does not explicitly require it.<br>• A Critical Cyber Asset may be part of a system or network, including other cyber assets, which is currently addressed somewhat by the ESP.<br>• The standards do not address interdependent functions across ESP boundaries, which may be essential to the Critical Cyber Asset and/or the BES. |
| ***Options*** | 1. Need to include both Critical Cyber Assets and critical functions.<br>2. Need to include an impact assessment of the components required for the critical function.<br>3. Need to include consideration and protection for interfaces into the Critical Cyber Assets – may be at a different risk level.  Protection may be required outside of the ESP. |
| **B** | **Not Protecting Assets Needing Protection** |
| ***Description*** | Assets which may have an impact on the BES, either singly or in conjunction with other assets are not being identified under CIP–002. |
| ***Comment*** | • Compliance with the NERC cyber security standards is onerous. |

- There are large penalties for non–compliance.
- Criticality based on BES system planning models (e.g. PSSE) are not adequate. BES interconnectivity and interdependencies are very different from cyber connectivity and interdependencies.
- Area requirements or impacts may not be available or considered in the identification of Critical Assets and Critical Cyber Assets (e.g. generation units' impact on the reliability and operability of the BES in a geographical area).
- Perception of "missing Critical Assets" creates a lack of confidence in the industry to self–manage.

***Options***

1. Include some responsibility for the BA in determining Critical Assets based on area impact (area overview).
2. Single largest contingency must be included in the impact / Critical Asset identification.
3. The Identifying Critical Assets Guideline[1] provides detailed guidance for Critical Asset evaluation.
4. Targeting specific risks / impacts can help focus the protection requirements.

**C** **Gaming**

***Description*** Entities are striving to create minimal or null Critical Asset Lists to avoid the effort and expense of complying with the standards.

***Comment***

- Some entities are taking a very literal interpretation of the standards, and some oppose guidance that is not explicitly included in the standards.
- Asset identification by some entities has been perceived as "unreasonable" and generated criticism of the industry.
- All compliance avoidance (gaming) cannot be completely anticipated or eliminated.
- Gaming will occur regardless of the methodology or framework applied. These issues can be addressed over time through the audit and compliance enforcement process.
- "Zero tolerance" for non–compliance: self–report a violation and possibly be fined (compliance culture vs. good security practice)

***Options***

1. Improve clarification of the intent of the standards and the requirements.

**D** **All or Nothing**

***Description*** Assets or cyber assets are either critical and require protection, or not critical and do not require any protection.

***Comment***

- Conducted diligently, including the interdependencies of systems required for essential functions, the asset identification can provide an adequate level of security for the BES.
- NERC's mandate is to protect the BES. This does not include distribution and the related assets.

[1] The NERC Guideline "Identifying Critical Assets" is presently under development by the Critical Infrastructure Protection Committee Risk Assessment Working Group. The development of this guidance document was directed by FERC in its NOPR, and reconfirmed in FERC Order 706 p253.

- There are no graduations or levels of assets, and no levels of protection for cyber assets.

***Options***

1. The fundamental tenet of the NERC reliability standards is to protect the reliable operation of the BES; therefore the focus of cyber protection, for both BES assets and cyber assets, should be on their impact to the reliable operation of the BES.
2. The Identifying Critical Assets Guideline1 provides some criteria to help define impact to the BES.
3. There may be a need to define what systems beyond the current Critical Assets need protection.
4. Required protection of cyber assets may be related to some characteristics (contains an operating system / purpose–written software / no software).
5. Multiple levels of protection do exist in the standards: critical cyber asset vs. non–critical cyber asset in an ESP vs. cyber asset outside an ESP. May want to provide a different granularity.
6. Define the breadth and depth of protection.

**5** **Loss of Asset – Integrity / Misuse**

***Description*** Determining the criticality of BES assets tends to focus on a loss (outage) of the asset. Loss of data integrity or misuse of the cyber assets may not be considered.

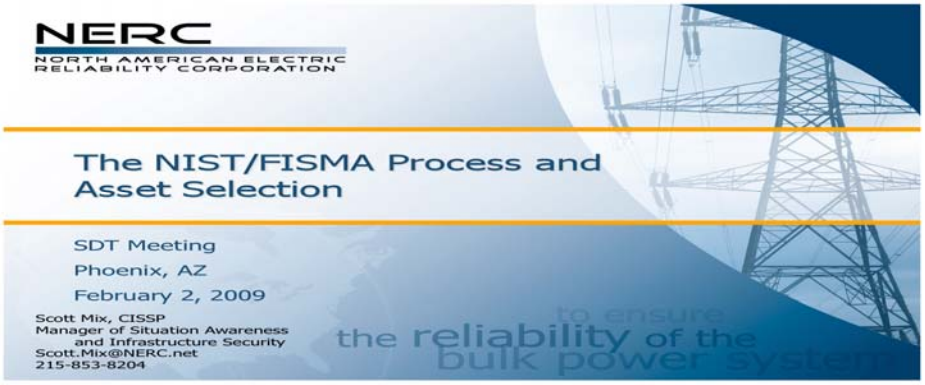
***Comment***

- Loss of an asset is a traditional risk analysis approach which may be incomplete for cyber impacts.
- Can be combined with other system or cyber events, increasing the impact
- Need to include the analysis of intentional and unintentional misuse.

***Options***

1. Consider magnitude of impact of loss of data integrity / misuse:
   - Generation or Transmission Control Centre – possible impact.
   - Transmission Substation or Generation Assets – little or no impact depending upon the size or function of the facility. May be related to the single largest contingency.
   - ISO – possible impact.
2. Need to educate industry to consider intentional and unintentional misuse

## Scott Mix, Strawman — FISMA Asset Selection



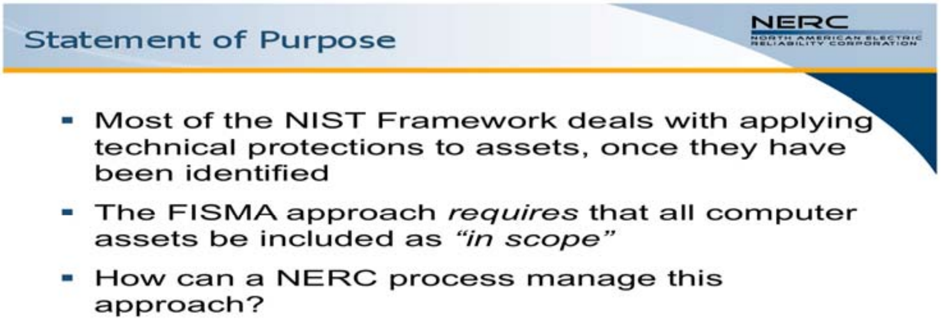
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

### The NIST/FISMA Process and Asset Selection

SDT Meeting
Phoenix, AZ
February 2, 2009

Scott Mix, CISSP
Manager of Situation Awareness
and Infrastructure Security
Scott.Mix@NERC.net
215-853-8204

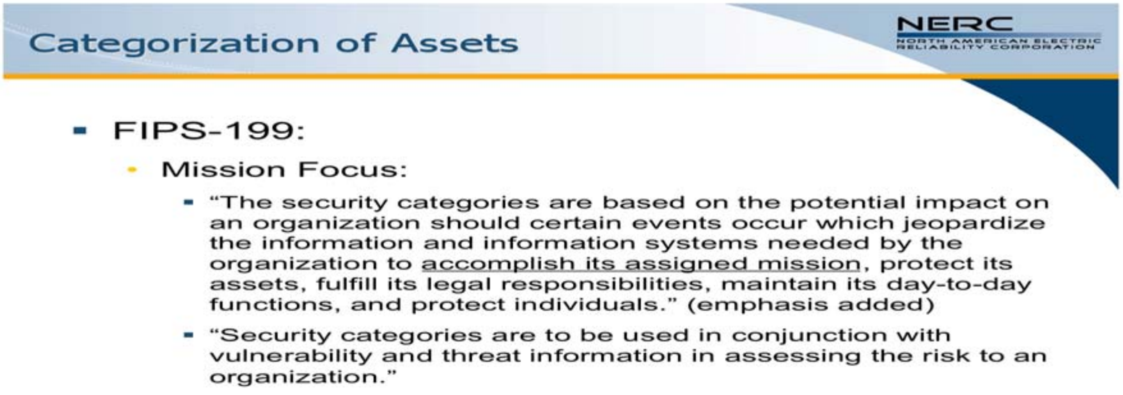
to ensure
the reliability of the
bulk power system



### Statement of Purpose

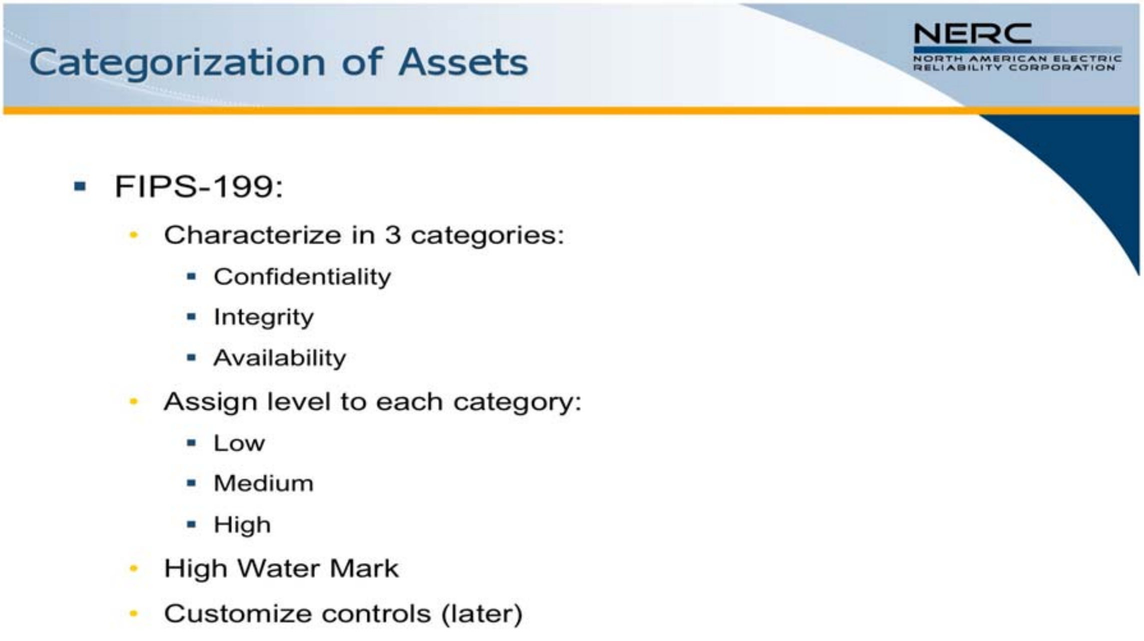
NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

- Most of the NIST Framework deals with applying technical protections to assets, once they have been identified
- The FISMA approach *requires* that all computer assets be included as *"in scope"*
- How can a NERC process manage this approach?



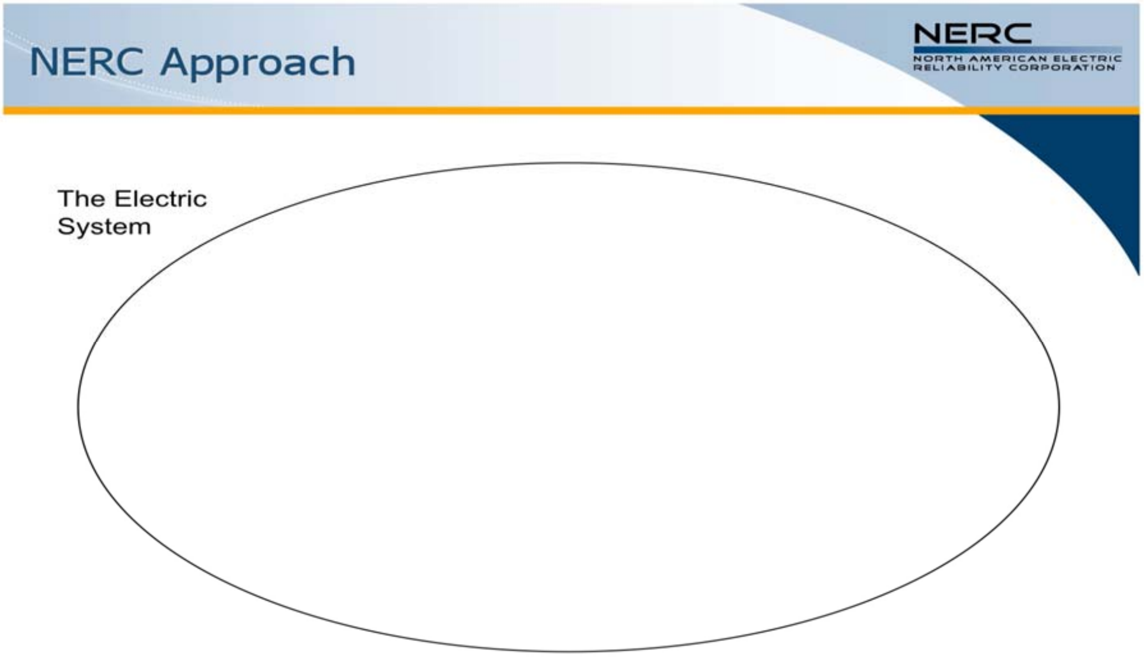
## Categorization of Assets

- FIPS-199:
  - Mission Focus:
    - "The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals." (emphasis added)
    - "Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization."



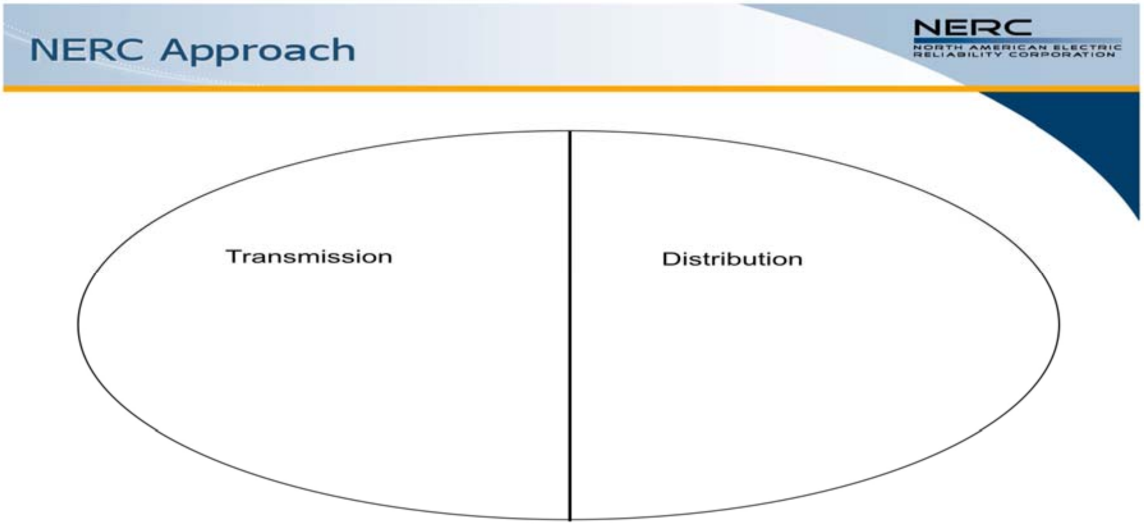
## Categorization of Assets

- FIPS-199:
  - Characterize in 3 categories:
    - Confidentiality
    - Integrity
    - Availability
  - Assign level to each category:
    - Low
    - Medium
    - High
  - High Water Mark
  - Customize controls (later)



## NERC Approach

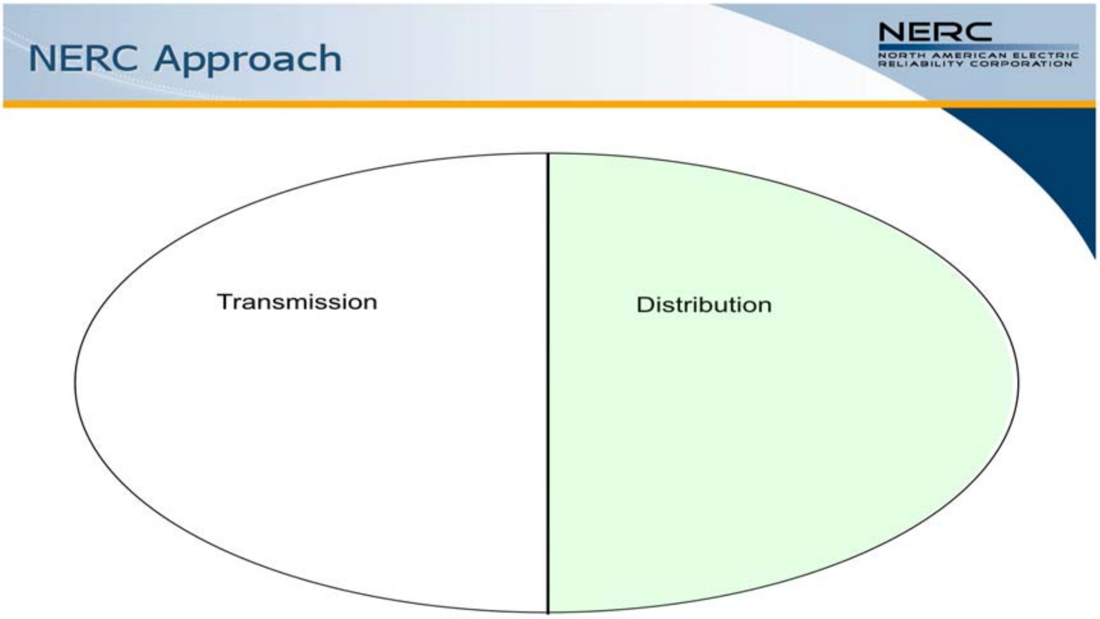
The Electric System



## NERC Approach

Transmission

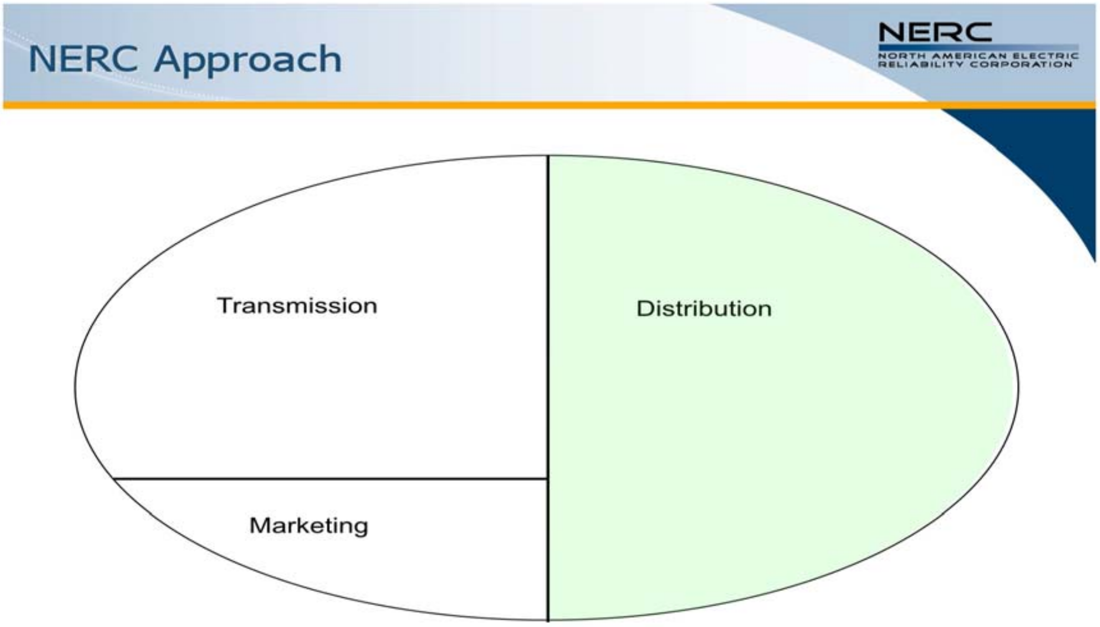
Distribution



## NERC Approach

Transmission

Distribution

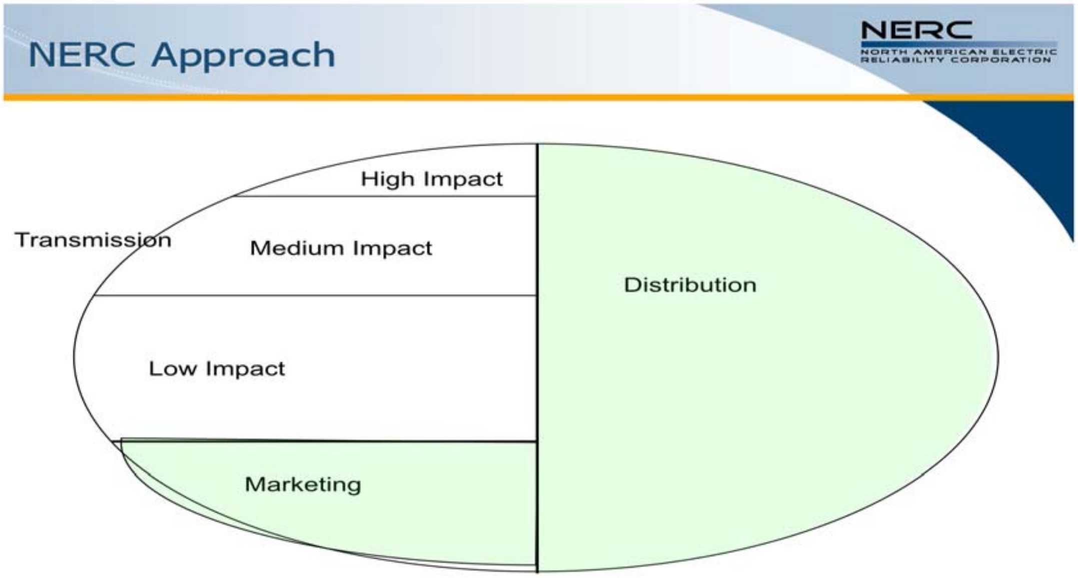


## NERC Approach

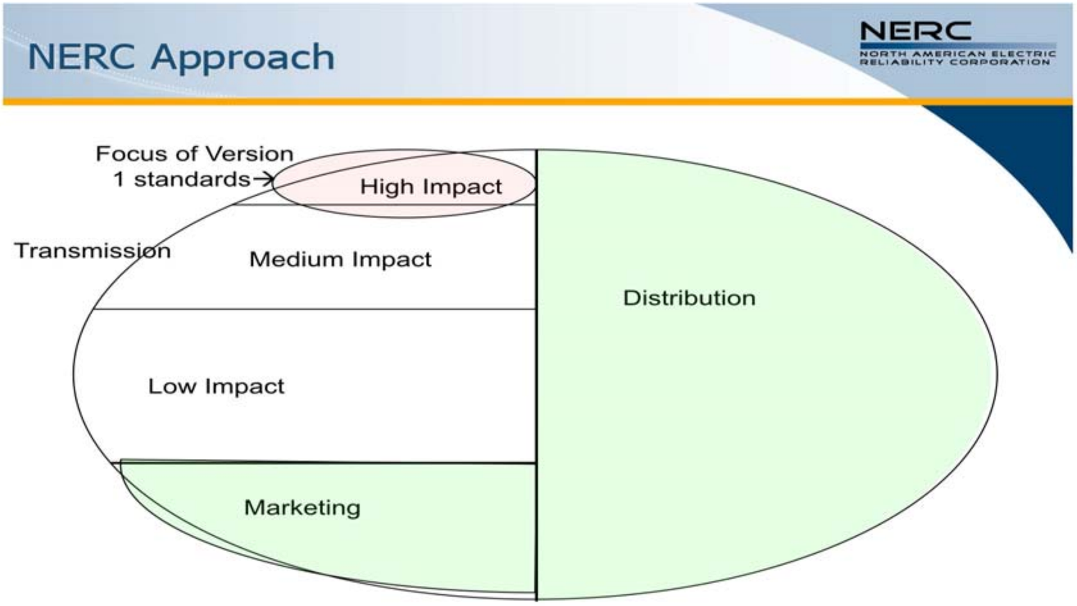
Transmission

Distribution

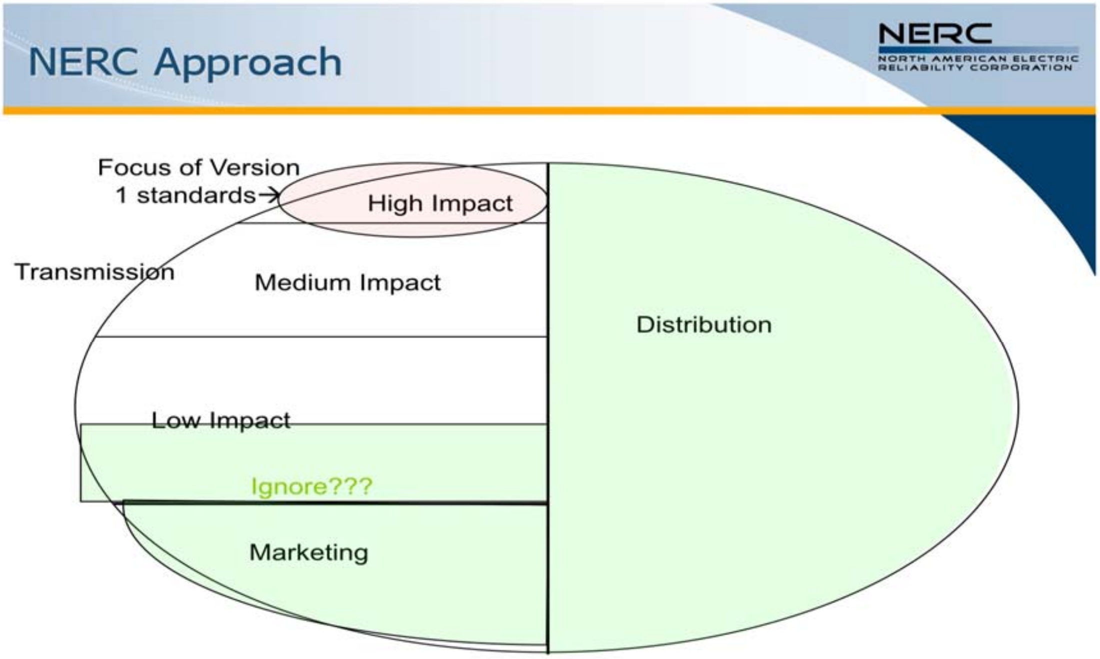
Marketing



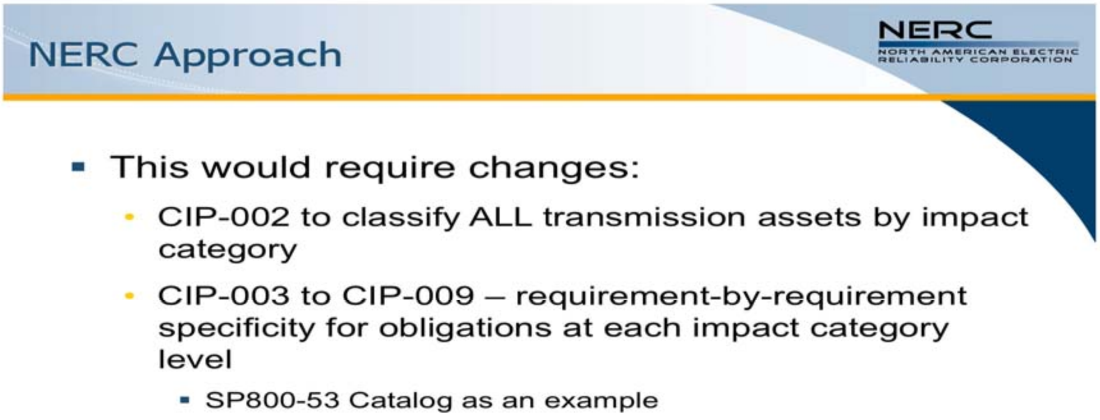
## NERC Approach



## NERC Approach

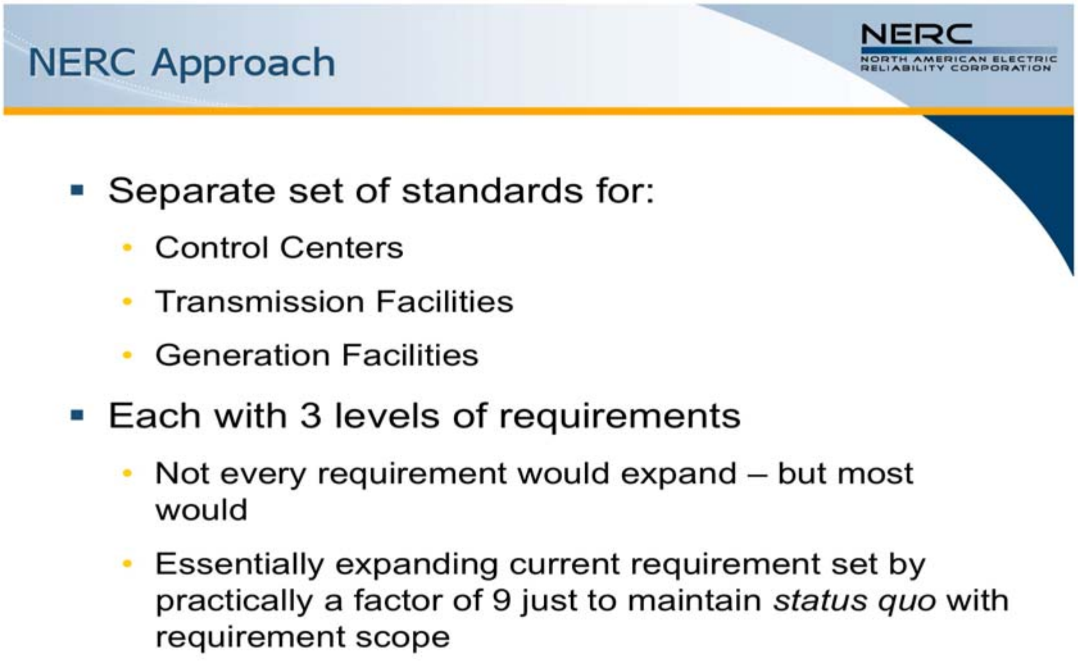


## NERC Approach



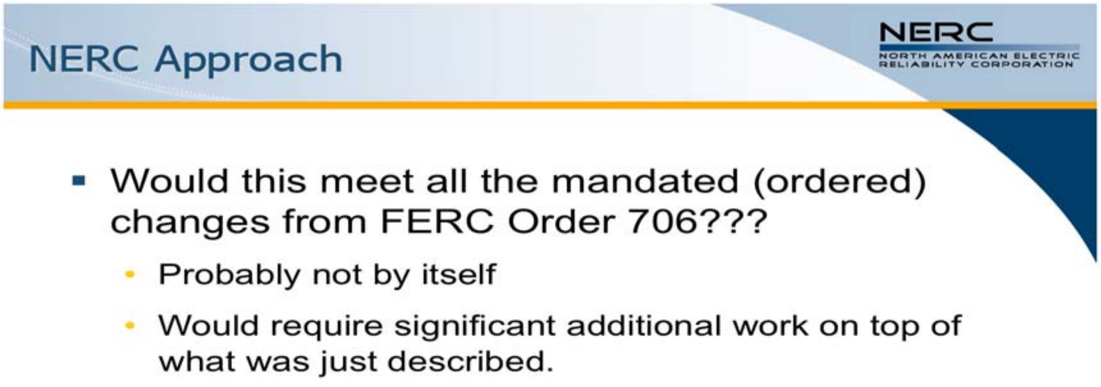
## NERC Approach

- This would require changes:
  - CIP-002 to classify ALL transmission assets by impact category
  - CIP-003 to CIP-009 – requirement-by-requirement specificity for obligations at each impact category level
    - SP800-53 Catalog as an example



## NERC Approach

- Separate set of standards for:
  - Control Centers
  - Transmission Facilities
  - Generation Facilities
- Each with 3 levels of requirements
  - Not every requirement would expand – but most would
  - Essentially expanding current requirement set by practically a factor of 9 just to maintain *status quo* with requirement scope



## NERC Approach

- Would this meet all the mandated (ordered) changes from FERC Order 706???
  - Probably not by itself
  - Would require significant additional work on top of what was just described.

**Appendix # 6**

## 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 percent acceptance or support of the members present is not achievable, final consensus recommendations will require at least 75 percent favorable vote of all members present and voting. This super majority decision rule underscores the importance of actively developing consensus throughout the process on substantive issues with the participation of all members. In instances where the team finds that even 75 percent acceptance or support is not achievable, the team's report will include documentation of any differences as well as the options that were considered for which there was greater than 50 percent support from the team. The team will develop its recommendations using consensus–building techniques with the leadership of the Chair and Vice Chair and the assistance of the facilitators. Techniques such as brainstorming, ranking and prioritizing approaches will be utilized. The team's consensus process will be conducted as a facilitated consensus–building process. team members, NERC staff and facilitators will be the only participants seated at the table. Only team members may participate in consensus ranking or vote on proposals and recommendations. Observers/members of the public are welcome to speak when recognized by the Facilitator and all written comments submitted on the comment forms will be included in the team and facilitators' summary reports.

The team will make decisions only when a quorum is present. A quorum shall be constituted by at least 51 percent of the appointed members being present (simple majority). The 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 percent supermajority voting requirement will supersede the normal voting requirements used in Robert's Rules of Order for decision making on substantive motions and amendments to motions. In addition, the Council will utilize their adopted meeting guidelines for conduct during meetings. The Council will make substantive recommendations using their adopted facilitated consensus–building procedures, and will use Robert's Rules of Order only for formal motions once a facilitated discussion is completed.

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

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

**Meeting Guidelines for Participants**

**Participants' role in meetings:**

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