NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

27th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Adopted by the SDT November 18, 2010

Toronto, Ontario

October 12, 2010, Tuesday - 8 AM to 6 PM EDT
October 13, 2010, Wednesday - 8 AM to 6 PM EDT
October 14, 2010, Thursday - 8 AM to 6 PM EDT

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CSO706 SDT October 12-14, 2010 Meeting Summary Contents

Cyber Security Order 706 SDT- Project 2008-06
27TH MEETING
October 12-14, 2010
Toronto, Canada

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Toronto and thanked Rob Antonishen at Ontario Power Generation for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines. On Wednesday morning, the SDT unanimously adopted the September 8-11, 2010 Winnipeg meeting summary and the September 15, 2010 SDT Conference Call Summary. On Wednesday at noon, the Chair, on behalf of the SDT, bid Jackie Collett a fond farewell and thanked her for her leadership and contributions. She will be taking a new position with Manitoba Hydro and will step down from the SDT in December 2010.

Bob Jones briefly reviewed the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting and sent to the Standards Committee in September. The schedule calls for a draft standard for formal comment to the industry by July 2011. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011. He also reviewed the CIP 002-4 schedule. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot.

In updates, Scott Mix, NERC noted the comments received were substantial for CIP 005-4 (over 200 pages) and he summarized common themes. The SDT is treating the posting as an informal comment process and plans to have revisions to the proposed standard by next week and a guidance document was posted in the meantime during the ballot period. The intent is to have this out for ballot along with CIP 002-4. Scott also noted that Jim Brenton, a member of the CAN-5 team, was not able to participate in the Toronto meeting and offered a brief report on the efforts to date. Finally he noted that the CAN-7 is technically completed. Dave Norton reported on NESCSO/NETL this new organization that has been funded by DOE and formed to address best practices with an academic flavor. Apparently two organizations have received DOE 3- year funding: EPRI and Energy Sec a small organization that meets once a year and has established a portal and secure chat facility. Howard Gugel reported on the NERC annual standards meeting in St. Louis and his presentation on the CIP work of the SDT. He noted there were questions about protecting assets (E.g. 69 KV in swamp) and small entities expressed concerns about the thresholds and he suggested that the SDT consider including information on why were are making transition to protecting all cyber assets on this up front in their next posting. Scott Mix reported that FERC has issued an order accepting the TFEs with some clean up and additional obligations and NERC will file another compliance filing in the next 90 days (Docket # RR 10-1-001). Howard Gugel reported that CIP 002-1 Declaration of Critical Assets, Balloting for Interpretation had closed but results not yet available.

The SDT reviewed the questions posed regarding CIP 002-4 on the September 29 Webinar and reviewed and refined responses for each question as a way to prepare for the challenge in responding to industry comments on the first ballot of CIP 002-4 in November. Howard Gugel, NERC staff, reviewed with the SDT a few changes agreed to by the SDT in that were inadvertently left off of the formal 45 day comment filing and he proposed, and the SDT agreed, to post a new CIP 002-4 version with errata corrected for balloting.

Dave Norton provided a review of the Framework Team's efforts to date, including several conference call meetings since it was created at the August SDT Chicago meeting. Their charge was to develop a framework strawman for the CIP framework going forward in 2011. He noted that the Team has begun to develop some documents including: a draft communications plan (Dave Revill), a rationale paper (Phil Huff), a spreadsheet with current requirements (Jay Cribb and Phil Huff) and a set of critical issues (Dave Norton).

Dave Norton presented a power point with six draft premises designed to stimulate SDT discussion on a framework going forward. The Team discussed and provided some potential responses for each of the premises:

- Premise #1, focusing on whether to assess the threats and risks or applying best practices against known vulnerabilities included discussion of: what threats are we defending against; reliability standards; audit-ability the nature of the framework; controls and "considering" the NIST; requirements and controls; and risk Assessment. In discussing this premise, the SDT concluded their approach will continue to be apply best practices against known vulnerabilities.
- Premise #2, focused on whether to take a minimalist or a transformative approach to the CIP standards concluded that this is not "either/or" but rather "both/and."
- Premise #3, focused on how the Team should respond to the directive to "consider" the NIST security risk management framework, and the discussion covered topics of: requirements language, TFEs, programmatic approach to standards drafting; compensating measures and a lesson learned culture. The Team concluded that this, like premise #2, may not be "either/or" but rather "both/and" and that "consideration" of NIST is not the same as adoption of NIST. The industry and the SDT should consider what aspects of the NIST approach fit the requirements model and whether adopting a programmatic approach to drafting standards will help to address the consideration of NIST.
- Premise # 4 focused on categorization of critical assets and the SDT generally concluded that both electrical impact and cyber security views should inform the standards and that trying to distinguish between high, medium and low may not be the best approach to providing cyber protection of the BES. The differences between transmission, generation and control centers may prove be more important than distinguishing H/M/L.
- Premise #5, focused on characterization of asset classes for protection and the SDT discussed physical security and its relationship to the characterizations and generally conclude that the three set paradigm should be the one to build on for the CIP.
-

- Premise #6 focused on whether and how standards should address the different genre and age of control equipment in terms of vulnerability, device class or technology.

On Thursday the Team developed a set of framework guidance statements based on the discussion. Phil Huff offered an initial draft of statements which the Team reviewed, refined and agreed to. Below are the final statements.

Ultimately, we need more structure in the requirement drafting process. The Framework Sub-Team's deliverable in December should be very concrete and clear in the proposed direction moving forward.

1. The Framework Sub-Team will develop a framework (e.g. style guide) for writing program-based requirements, where appropriate. This framework should include:
   - Minimizing zero-defects in compliance requirements
   - Guidance for rationale statements for individual requirements that speak to the vulnerabilities they address.
2. The Framework Sub-Team will develop a high-level narrative to answer the foundational question of "What are we trying to protect against?"
3. The Framework Sub-Team will develop a model which applies a baseline set of requirements for all BES Cyber Systems which allows for enhanced requirements for:
   - High impact
   - Specifications for generation, transmission, and control centers
   - Specifications for legacy vs. state-of-the-art equipment
   - Connectivity considerations
4. The Framework Sub-Team will consider developing a framework for incorporating vulnerability assessments into the current standards for the purpose of allowing flexibility in applying security controls.

Following the discussion of the premises and prior to refining and finalizing the guidance statements, the SDT discussed the following issues related to the development of the framework: manage security like reliability; change the zero-defect approach; change the industry approach to self reports; improve uniformity of audits.

The Framework Team has been asked to provide a draft answer the question of the organization of the CIP going forward and has been developing a clearer documentation of the rationale for the changes reflected in the draft CIP 10 and 11. The Chair asked each SDT member, through a round-robin review, to describe their current thinking on the format for the CIP. He noted that at its Sacramento meeting the SDT was nearly evenly split on the format question. Several members noted they had changed their earlier position supporting the use the existing CIP 003-009 format and many now said that form should follow function and that either format approach, or even another format approach would be acceptable. The facilitate summarized the results of the exercise suggesting there was in evidence a lot more openness

around this issue than in Sacramento and a shared value of getting the requirements right first and then organizing the format and that the Framework Team could focus on the goal of eliminating or reducing cross-linking in the standard requirements and TFEs. The Chair suggested the Framework Team continue its efforts in preparing a strawman for the December, 2010 meeting in Orlando. He also noted that the communication plan for industry outreach and education that the Team is developing will be critical to the success of the SDT.

The Team reviewed the steps and assignments coming into the Baltimore meeting. The SDT agreed to engage in a series of conference call meetings (Monday-Friday, 11:00 a.m.-3:00 p.m.) the week before the Baltimore meeting to review industry comments and review and refine a set of strawman SDT responses to the comments. Tom Stevenson provided an overview of Constellation Energy's facility in Baltimore where the SDT will meet in November. The Chair thanked Rob Antonishen for his excellent hosting of the SDT in Toronto.

The meeting adjourned at 4:40 on Thursday

_____

Cyber Security Order 706 SDT- Project 2008-06
27TH MEETING SUMMARY
October 10-12, 2010
Toronto, Canada

I. AGENDA REVIEW, WORKPLAN SCHEDULE AND UPDATES

A. Agenda Review and Adoption of Meeting SDT Summaries

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Toronto and thanked Rob Antonishen at Ontario Power Generation for hosting the meeting. Rob covered logistics. Howard Gugel, NERC, conducted a roll call *(See Appendix #2)* and reviewed the antitrust and public meeting guidelines *(See Appendix #3)* with the meeting participants at the outset on each day. On Wednesday morning, the SDT unanimously adopted the September 8-11, 2010 Winnipeg meeting summary and the September 15, 2010 SDT Conference Call Summary. John Lim reviewed the proposed meeting objectives, the facilitator Bob Jones reviewed and the SDT agreed to the proposed timed agenda. On Wednesday at noon, the Chair, on behalf of the SDT, bid Jackie Collett a fond farewell and thanked her for her leadership and contributions. She will be taking a new position with Manitoba Hydro and will step down from the SDT in December, 2010.

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

Bob Jones briefly reviewed the schedule for CIP 010 & CIP-011, which was adopted by the SDT during the Chicago meeting and sent to the Standards Committee in September and calls for a draft standard for formal comment to the industry by July, 2011, meaning there are about 6 months starting in December for the SDT to complete this task. In December, the SDT will be reviewing the recommendations from the Framework Sub-Team and determining the course for the further development of the CIP standards in 2011.

He also reviewed the CIP 002-4 schedule. During the November meeting in Baltimore, the SDT will be reviewing and responding to industry comments and determining what changes to make to CIP 002-4 before posting for the 2nd ballot.

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

1. Update on Urgent Action CIP 005-4 process- *Scott Mix*

Scott Mix noted the comments were substantial on CIP 005-4 (over 200 pages). He summarized common themes. The SDT has had several conference calls to resolve issues (such as local definitions of remote access and other issues) and they are treating the posting as an informal comment process. He also noted that the new NERC version of standards development was recently approved by FERC

which removed urgent action and replaced it with an "expedited" process. The SDT plans to have revisions to the proposed standard by next week and a guidance document was posted in the meantime during the ballot period. The intent is to have this out for ballot along with CIP 002-4.

2. **Update on CAN 5-** ***Scott Mix***

Scott noted that Jim Brenton was not able to participate in the Toronto meeting. Scott offered a brief report on the efforts to date include a possible "misstatement" about operator laptop control.

3. **Update on CAN 7-** ***Scott Mix***

Scott noted that this CAN in technically completed.

4. **Update on NESCSO at NETL-** ***Dave Norton***

Dave Norton reported on this new organization that has been funded by DOE and formed to address best practices with an academic flavor. Apparently two organizations have received DOE 3- year funding: Energy Sec a small organization that meets once a year and has established a portal and secure chat facility; and EPRI. The conference was attended by a couple other SDT members (Jim Brenton and John Van Boxtel) and featured a presentation by Mike Assante on his work on professional certification.

5. **October NERC annual standards meeting in St. Louis-** ***Howard Gugel***

Howard Gugel reported on the NERC annual standards meeting in St. Louis and his presentation on the CIP work of the SDT. He noted there were questions about protecting assets (E.g. 69 KV in swamp) and small entities expressed concerns about the thresholds. He underscored the need to look at this from both an engineering and IT perspective and consider the threat of attack vectors and simultaneous attacks. He suggested that the SDT consider including information on why were are making transition to protecting all cyber assets on this up front in their next posting.

The SDT discussed what approach we are taking (bright lines or tailored protection), CIP 002-4 addressing the highest level of protection; the use of mutual distrust and small systems; and until the functional model changes, the SDT should write standards for what is in NERC's purview.

6. **Technical Feasibility Exceptions-** *Scott Mix*

Scott Mix reported that FERC has issued an order accepting the TFEs with some clean up and additional obligations and NERC will file another compliance filing in the next 90 days (Docket # RR 10-1-001). The SDT discussion covered: when will it take effect? A: after FERC approval; NERC has to file compliance filing to add those and other clean up. Until that 006 and 007 not subject; another

Appendix 4D filing will be done; how will the TFE process address applying a patch? A: Not sure yet lawyers are reviewing.

7. CIP 002-1 Declaration of Critical Assets, Balloting for Interpretation.

Howard Gugel reported on this ballot noting it has closed but results not yet available.

II. REVIEW OF CIP 002-4 WEBINAR QUESTIONS AND RESPONSES

The SDT reviewed the questions posed regarding CIP 002-4 on the September 29 Webinar and reviewed and refined responses for each question as a way to prepare for the challenge in responding to industry comments on the first ballot of CIP 002-4 in November. *See Appendix XX for the SDT discussion comments and final response statements.*

At the conclusion of the webinar, NERC offered to post the questions raised and responses offered as a resource for the industry to review in reflecting on CIP 002-4 when balloted. The SDT agreed to offer additional comments, where needed, to clarify any responses that team members offered during the course of the webinar.

Howard Gugel, NERC staff, reviewed with the SDT a few changes agreed to by the SDT in that were inadvertently left off of the formal 45 day comment filing including: deleting "senior officer"; deleting the exception for nuclear facilities in CIP 008; and 1.1 – "greater than 1500 MW" vs."1500 or more." which both should have been deleted. He proposed, and the SDT agreed, to post a new CIP 002-4 version with errata corrected for balloting. Members discussed the fact that the Guidance Document clarified that manually initiated was not automatic load shed and this should be consistent in CIP 002-4.

III. FRAMEWORK TEAM REPORT AND SDT DISCUSSION OF CRITICAL ISSUES

Dave Norton provided a review of the Framework Team's efforts, including several conference call meetings since it was created at the August SDT Chicago meeting. Their charge was to develop a framework strawman for the CIP framework going forward in 2011. Team members included: Dave Norton, Jim Brenton, Jay Cribb, Joe Doetzl, Phil Huff, Doug Johnson, Dave Revill, Jon Stanford, and John Van Boxtel. Mike Keane at FERC and Scott Mix at NERC also participated. He noted that the attendance has been spotty but the Team has begun to develop some documents including: a draft communications plan (Dave Revill), a rationale paper (Phil Huff), a spread sheet with current requirements (Jay Cribb and Phil Huff) and a set of critical issues (Dave Norton).

A. Review of Critical Issues and Premises

Dave Norton presented a power point with some framing premises designed to stimulate SDT discussion on a framework going forward. Howard Gugel noted that the Team had asked Keith Stouffer do a presentation on the NIST framework but he was unable to at this meeting. Keith agreed to do so at the December meeting or in a webinar format prior to that meeting. Jay Cribb suggested the question for the SDT was what "shade of gray are we going to choose?" Dave Norton noted his concern regarding the industry's ability to absorb these changes. The facilitator suggested that the goal of the review of these premises is not driving towards consensus but rather an opportunity for the SDT to flush out and discuss the issues.

Draft Premise #1`: Known vectors that threats can exploit are vulnerabilities. Risk is calculated impact measured as the product of financial loss X probability of exploitation. Risk is difficult to quantify in the case of widespread loss of critical electric infrastructure, except to conclude that it is unacceptable. Therefore:

1. Is rigorous formal syllogistic assessment of threats and risk a necessary prerequisite to drafting, or

2. Is prescription of generally accepted best practice controls and countermeasures for defending against known vulnerabilities satisfactory for writing CIP standards?

Dave Norton posed the following question: while the SDT won't write standards for unknown vulnerabilities, do we need to document how many bad things can happen? The SDT after an extended discussion concluded that it does not make sense, nor will it be possible for the Team to assess the threats and risks and that it should continue with the model of applying best practices against known vulnerabilities. Some consideration should be given to whether the SDT could add rigor to vulnerability threats by utilizing the knowledge of its members and going out to entities to take some informal sampling in order to reasonably conclude that the proposed controls are addressing known vulnerabilities.

Member and participant comments covered the following issues and questions:

- **What Threats are We Defending Against?** We need to clarify these.
- We have looked at threat vectors in building the CIP standards;
- Should we stay where we are with the application of standards protecting against vulnerability;
- The best practices approach makes sense since the top 10 threats have not changed that much from year to year.
- Should we protect for 90% and detect the rest?
- Some threats are not reliant on network connectivity.

- Current standards have threat and risk infused into them because if you have a requirement framework you must do this; in the NIST framework controls are set of tools not requirements, that provide guidance;
- We can't start with a threat assessment since we don't have ability to see every entity and determine which ones apply.
- Most of threats comes from inside which can be addressed by configuration management, awareness and training, Perimeter defenses are generally well designed but its the inner connectivity that gets us into trouble.
- For "advanced persistent threats", firewall defenses are not effective. There is lots of social engineering that goes into this.
- We have an opportunity since we still don't have a way of assessing risk. If we did, wouldn't be problems with these standards. Why not discuss a risk assessment methodology?
- Look at risk assessment for a sector- problem is models are wrong. DHS heavily terrorism focused.
- We are haunted by the risk of writing a cookbook for the bad guys if everything in the overall system is the same.
- We can identify the basis we are coming from and document our assumptions. The problem in over the past year, we have made decisions without a basis to go back to. The SDT needs to restate its assumptions when making applicability decisions.
- **Reliability Standards.** EPA 215 2005- one line: "reliability standard means a requirement". By law we have to focus on requirements and a NIST tailoring effort ultimately won't fit.
- Current CIP standards are not where they need to be and could be stronger. The SDT should make the changes in confines of the law.
- **Audit-ability** against the requirements needs to be addressed and how to address whether the current audit regime needs to be changed;
- Do auditable and measureable standards result in rigorously protecting from the threats;
- **The Framework.** The purpose of the framework is to develop risk assessment on behalf of the industry.
- NERC's framework didn't get the right things and left communication systems out.
- We should avoid an "all risks/all perils" as we can't protect everything. We should clarify what is the dividing bright line. Is it routable protocols?
- We need a narrative cover sheet laying out the elements of what we are doing. These controls map back to that exposure to risk.
- Not an organizational dynamic risk assessment. The narrative- should address this. Narrative to communicate this.
- We may have an opportunity to add rigor to our assessment of vulnerability threats by checking in with entities to informally test whether the proposed controls are addressing known vulnerabilities.
- If dealing with known vulnerabilities, we know that there will always be additional ones. Maybe focus on what to exclude and defend against everything else.
- **Controls and Considering the NIST.** We should talk about generally accepted core controls that apply to the risk and not apply the NIST catalogue. In the NIST catalogue there are too

many controls in the high category and many that shouldn't be in there. Take the NIST controls that have value and work well.

- **Requirements and Controls.** The value will come in providing requirements to apply in your environment that will address the risks without embarking on a NIST risk management approach.
- Need to continue with effort to allow and guide the industry to select controls that fit the environment. How do you determine this without assessing the risk? e.g. CIP 66. 1.1 Secure cabling within a center.
- The SDT needs a narrative (not scientific) map to allow tailoring of controls to the risks we are protecting against.
- We should firm up the under-penning of best practices and be more specific on technical areas where we need to.
- We have to use our collective experience look at the real risks to the BES. Not all threats are equal and too many controls is not a good thing. Currently we don't give enough guidance on how to tailor the controls in light of the weighing of risks.
- **Risk Assessment.** Is a formal assessment of risks a prerequisite? We may have this already ("coordinated means connectivity" from NERC's Report, Critical Infrastructure Strategic Roadmap)

Draft Premise #2: The first CIP SDT considered -003 thru -009 minimum requirements, and expected subsequent augmentative drafting efforts to improve them based on experience.

Should our fundamental approach be:

1. Minimalist: Treat existing standards language as "the" baseline and augment them per specific directives in Order 706, using SP800-53 for enhancement language? Or…

2. Transformative: Literally embrace the NIST paradigm and create new sets of controls for each technical subject area, likely organized differently from the current version?

How much change can the industry absorb? How fast?

Member and participant comments covered the following issues and questions:

- In discussing this premise, the SDT concluded that this is not "either/or" but rather "both/and."

Draft Premise #3: FERC directed the SDT to 'consider' use of the NIST Security Risk Management Framework, which permits use of alternative "compensating measures," and judges adequacy of controls and countermeasures in terms of overall "programmatic effectiveness."

1. Is it in the best interest of all concerned to transition to the NIST "risk management" approach to compliance? Or…
2. Is it better to continue with literal and binary requirement compliance language measurement? Can we infuse needed flexibility through careful crafting of VRF/VSL?

Member and participant comments covered the following issues and questions:

In discussing this premise, the SDT concluded that this, like premise #2, may not be "either/or" but rather "both/and." "Consideration" of NIST is not the same as adoption of NIST and the industry and the SDT should consider what aspects of the NIST approach fit the requirements model. Adopting a programmatic approach to drafting standards will help to address the consideration of NIST. Currently there are few rewards and clear punishment for self-reporting standards violations. This "fear of fines" should be addressed by both FERC and NERC to help develop a "lessons learned" culture within the industry. The standards should give the appropriate flexibility for companies to implement compensating measures like those in the NRC as well as the TFE process. - allows compensating measure and this is similar to TFE process. In drafting standards the SDT should focus on "overall programmatic effectiveness" which can create both technical (physical, electronic and technical) and procedural defense in depth.

Member and participant comments covered the following issues and questions:

- **Requirements language.** If we avoid making it a violation and find the right words for the requirements, we don't have to worry about assigning a VRF/VSL.
- The requirements language has to be binary. The requirements are the only thing the SDT has responsibility for. Industry does not vote for VRFs/VSLs.
- There probably isn't a framework for question #1.
- **TFE.** Industry can shed light on direction the SDT might consider going in terms of TFE. Which requirements should the TFE apply to. Compensating measures were asked for. This will require discussion with audit team.
- Note the "Safe harbor" provision in TFE- advanced knowledge and ability to predict what is happening in a compliance action.
- **Programmatic Approach.** A programmatic approach will make this easier and go a ways towards meeting the directive of "considering" the NIST.
- Does programmatic effectiveness = compensating measures?
- A program is not an approach. Documentation for compliance purposes to prove you are doing the steps and if you find a problem you have a feedback loop to catch, address and fix the problem.
- **Compensating measures** will be judged in an audit. Prove "as good as or comparable to."

- Feedback loop and requirements should be an iterative process. People are not supported and valued for doing it.
- **Lessons Learned Culture.** Write good clear standards and provide guidance to help. The system should support with a "lessons learned" culture and a change in the audit approach.
- The FERC 706 Order directs the Team to "consider NIST framework."
- In our first draft, lows had 30% of the requirements, which was not viewed well.
- Are we focusing on risk management vs. the NERC binary compliance model?
- Can we infuse any flexibility into VRF/VSL? To drive constant improvement?
- What is a program approach? If you miss something but other controls caught that and corrected. That is a program approach to defense in depth. More complicated and you are layering standards to compensating and mitigating.
- Agree with this but it is hard to write this in as a requirement. When requirements went from voluntary to mandatory and enforceable – lawyers and executives have been telling what these words meant.
- Model is based on fear in CIP 002 R1 and R2- $1 million a day fines. NERC and FERC have to help and get truth out to the regions.
- FERC has to help. Commission has to say we understand- tone this down. If everyone wasn't scared for penalties. That's why minimized everything out of CIP 002.
- We (NERC and FERC) need to help each other. 80/20%. Thinking outside the box moving the platform forward. How to move best practices forward. Provides more of a conversation. We will get more polarized if we go that route. Doesn't see the 215 language is quite as restrictive.
- The law shouldn't prohibit this expertise. For Versions 1-3 the requirement was for a risk-based methodology.
- The second option is on enforcement not audit side.
- Technical people at FERC are very grounded and balanced. We need a little more outreach to address the fact that the guy writing the "self report" gets fired.
- The Federal definition of IT is very expansive.
- Version 1 CIP- risk assessment- what is the risk to BES of the asset. Use judgment to decide what controls to add.
- The standards should give the appropriate flexibility for companies to implement compensating measures. E.g. NRC- allows compensating measure and this is similar to TFE process.
- Standards- "overall programmatic effectiveness" – this creates both technical and procedural defense in depth. Can be physical, electronic, technical, procedural
- 40,000 every 7 years. Built in compensation for extra level of risk and institute program for catching errors (feedback loop).
- Enforcement- $$ amounts. NERC website. Fines that have gone through the process. The magnitude should persuade this is not the problem it is made out to be. They are rational and reasonable.
- We need to look at how many ways can we look at the "consider"- different pieces of the NIST approach we might use without using all.

- FIPS 199 and 200. Starting with systems- from control to payroll and communications. Evaluate sensitivity of this system to your mission (confidentiality, integrity availability). Very different in the federal context.
- Electric is the hub of many other systems and we are charged to keep it going. This is up high in terms of criticality.
- Bonneville's only high is a control center.
- Mission is to keep the lights on for BES. Control security vs. information security
- CIP 10- take model of FIPS 199 and its impact to mission. Assumptions about mission and impact levels. It would be Electric power system customization of the FIPS 199 process. (not a CIA but an AIC mapping)

Premise #4 Categorization: Destabilization of the BES through cyber/hybrid means requires simultaneous, successfully debilitating attacks on CCA at multiple CA locales.

Critical Questions/Options

1. If so, is size-based CA categorization the key differentiator in cyber security engineering? And, if so, what are the 'bright line' size demarcations between High/Medium, and Medium/Low; or High/All Else?

2. If not, what is the key differentiator(s) in cyber security engineering for protection of the BES, and is categorization of this differentiator appropriate or necessary? How?

The SDT agreed that both electrical impact and cyber security views should inform the standards and trying to distinguish between high, medium and low may not be the best approach to providing cyber protection of the BES. The difference between transmission, generation and control centers may be more important than distinguishing H/M/L. Navigability to the control host may be the key and boundary protections and zone of control remain very important as a fundamental concept.

Member and participant comments covered the following issues and questions:

- We need to focus on how bad guys navigate in networks.
- **H/M/L.** When H/M/L came up before we discovered it was hard to put medium definitions in. Liked it as a concept but in talking with security people, they think it will be very difficult to implement.
- The problem the SDT has faced after high, is where is the medium and low.
- H/M/L may be too complex. Move to two tiered. Real difficult to say what is a medium.
- H/M/L – moderate/medium won't work well. Lows are getting controls inherited.
- High and other? Other will take care of your base programmatic controls. Works out better to standardize with one base and train to that.
- We have been focused on high to date. Now if we say in two tiered. Look again at controls
- "Scope of impact: "- 500 kv with lots of things. 100 69 kv connected IP. Combines both-engineering view of electrical impact and cyber security view of how much stuff could I do

because of connectivity, age of equipment. Might bring more under the tent. Will be a complicated method of arriving at where you need to do what.

- **Big iron** is used to assess impact. Limits you cyber security scope. In NIST is impact to your agency. Risks can be inherited. Interconnectivity.
- Look at defining violation levels. High= interconnectivity?
- Maybe a baseline with enhancement for high impact. Facilities by themselves with an impact vs. those in combination with others.
- How much change can people take each time? Every year? 3-5 year. Precedent of changing the structure. Have the high coming in and supplement. CIP 002-4 sets high mark. Come in next time to set baseline.
- **Complexity.** The SDT released its concept paper in mid-2009 which was 2 dimensional- BES and cyber impacts and the industry said too complex.
- In favor of keeping 10 in terms of impact.
- Same criteria as attachment 1? Baseline requirement- change management, password protection. What will be layered on that? This will increase in assets coming under scrutiny.
- Need to make sure there are some could have something that is not high. E.g. 69 kv. owned by one company. No impact on BES.
- There is something in low that is not apparent. Some apply to the RE and not to the asset. Lot of inefficiency of current standards. We could make apply uniformly to RE even if you have small assets. Programs for the future.
- What do you have for physical security, personnel security etc.
- Pin to a company or to their function in the functional model? NERC does not control certain aspects in industry. It should at least be tied to NERC functional model.
- We are looking to have a common set of controls that apply to all. If you are in set of entities that CIP standards apply to then you will implement common controls.
- BES cyber systems is the universe within which we need to develop standards.
- The difference between transmission, generation and control centers may be more important than H/M/L.
- Transmission communicates with a control center and locally and unmanned (except for maintenance)
- Generation- manned more often (generally). Different criteria with security already embedded. They talk with control centers or with other generation sites.
- Control centers talk the most with other entities and need layers of protection. Highest around controls around control center, less around field assets.
- Vulnerability back to control center- whether in swamp or big generator.
- This may be more effective than to think about high/medium/low.
- Navigability to the control host is the key.
- What about mini-data center in the substations- bunch of control centers. Scope of impact less. Creating new set of sub-stations.
- What should the entity consider in making decisions on selection of controls?
- Framework should provide the parameters for the drafters in putting together controls.

- Considered going through each of requirements and listing the parameters. Look at organizational security requirements that should provide across the board/ BES.
- Look then at operational and technical controls and consider some of the characteristics based on environment (generation, transmission, control centers) and make distinctions on how to apply.
- Does the size of the asset connected to control center determine whether and how to protect the center?
- Connectivity- it is an attack vector that the spot needs to address.
- We should focus on the sake of BES security and not for protecting computer systems.
- Boundary protections and zone of control remain very important. This is fundamental concept.
- Thinking about to my control hosts and syncro-phasers.

Premise #5- Characterization Asset Classes: The first CIP SDT considered -003 thru -009 to be foremost applicable specifically to control system hosts and operator consoles at work in data/control centers. They did not expect CIP V1 to be applied to field assets without adaptation.

Critical Questions/Options

1. Should we adopt a two tier paradigm; in essence writing <u>two sets</u> of standards as appropriate for:
   a. Bastion sites: generating plants and data/control centers, and,
   b. Distributed Field sites: Substations, dams, etc.?

2. Or, a <u>three set</u> paradigm, specific to each: 1) Generation 2) Transmission 3) Control Centers?

The SDT agreed that the three set paradigm should be the one to build on for the CIP.

Member and participant comments covered the following issues and questions:

- Generation, transmission and control centers set the paradigm. Define the baseline and break out three sets.
- This turns on physical security- use this a compensating measure. Does it give us an out?
- **Physical security** is most difficult issue we have to deal with. Many utilities use distribution personnel as first responders. Toughest nut to crack is to use as compensating measure to ensure you have access control, etc. Direction industry needs to go. Difficult going forward. Unintended reliability contact.
- How can we use this physical security as a tool
- Physical security- bastion/distributed field sites- makes sense.
- This should be a tool to mitigate risk. Some modicum of physical security should exist. E.g. security reviews on annual basis.
- CIP only addresses critical cyber asset. This level of security at the lows- puts at whole different level.
- We can bleed these together as a both/and: Bastion/distributed field and generation/transmission/control centers.
- This would make it more complicated as it is hybrid of the two- physical and electronic.

- Devil is in the details. Useful tool to include- G/T/CCs- with 3 different standards?
- Could bastion equate to high? Big substations as bastions/ high. Variations on 3 - G/T/CCs.
- Provide requirements in areas of physical security that describe what your are trying to protect against. Provide security controls. Have utility determine what compensating are equivalent.
- Remove high from geography. Don't care where it is sitting. Scope of impact. The most critical sub-stations. May not be a high- function.
- Cyber system focus-what is the cyber system and what it can do.
- What is the amount of protection required? Not impacted as much as this needs high level of protection. What level of protection do you want to apply physical/electronic?
- Some teams were writing in the G/T/CCs in this approach.
- Direction- we are in agreement with the direction heading in the first place.
- Do we need some granularity in terms of devices out there?
- In practice look at all requirements on CIP 10 and 11. Little differentiation in using these concepts. There is a difference in environments which should be taken into account.
- Is it really environmental or is it at the component level.
- Framework team to put some structure around this. Define a little better and structure it so it is more formal and consistent. Express those and formalize somewhat in a document to hand off to the sub-teams in order to get some uniformity.
- Reason this didn't get separated into G/T/CCs is it is missing the general narrative regarding what we are protecting against. Are we protecting against everything everywhere? This will lend it self to creating differences and nuances to different environments.
- Does the programmatic model lend itself to a more general approach
- Some programmatic areas depend on the organization and it won't matter in terms of context/environment and where it connects to the assets. Use enhancements only where needed.
- This isn't a fair characterization of Version 1 SDT.
- Expected the auditors to take care of this. Lawyers insisted it to be verified.

Premise #6 Different Genre/Age of Control Equipment: CIP V1 did not take into account differences in the genre and age of controls equipment; resulting in "one size fits all" requirements that are inadequate for protecting some subsets of CCA and overkill for others, and the apparent cause of the need for many TFE.

Critical Questions/Options

1. Do we need to write different standards requirements for different genre and ages of control system/IED?
2. If so, how shall we parse the different genre and ages of control system/IED? What are the 'bright lines'?

Member and participant comments covered the following issues and questions:

- The Sub-team has struggled this. CCA gets a package of stuff dumped. (or next to CCA).
- BES cyber system ("target of a "plop")

- What are the device classes we can make applicability judgments that make sense.
- It is the technology: routable, serial, type of communication vs. class of device?
- We should take care in "communications" Is it an issue of the type of system? What differentiation of a device that will determine the type of controls.
- Do we go to granular level on vulnerability issue regarding those devices?
- Do we have the sub-team do the more granular vulnerability assessment piece? Yes.
- We will need to address this at the controls level by each sub team.
- How do we determine the classes of device to apply the controls?
- We need a classification model from the Drafting Team.
- Fragility caused by complexity and connectivity.
- Better approach- consider the characteristics of each device applicable to each individual requirement. 'general purpose operating system.' (e.g. networking requirements- how device communicates, etc)
- Everything has such a system. Knowledge there just not readily available.
- We missed an opportunity to impose on vendors- they should participate in this. Entities trying to educate- kick. Need government to step in.
- Protect against pieces of equipment used for purposes other than they were designed to. What other things can be done with the piece of equipment.
- National SCADA test bed program. Procurement document. That won't help us here now on this one.
- Premises regarding V1- SDT- were addressed but implementation and crafting of final requirements.
- E.g. TFE came in as different ages of equipment. Wouldn't have been introduced.
- Didn't believe this was going to the field.
- Attempted to address and failed miserably. We got to fix next time around.

B. Final SDT Guidance Statements for the Framework Team

On Thursday the Team developed a set of framework guidance statements based on the discussion. Phil Huff offered an initial draft of statements which the Team reviewed, refined and agreed to. Below are the final statements.

Ultimately, we need more structure in the requirement drafting process. The Framework Sub-Team's deliverable in December should be very concrete and clear in the proposed direction moving forward.

1. The Framework Sub-Team will develop a framework (e.g. style guide) for writing program- based requirements, where appropriate. This framework should include:
   - Minimizing zero-defects in compliance requirements
   - Guidance for rationale statements for individual requirements that speak to the vulnerabilities they address.

2. The Framework Sub-Team will develop a high-level narrative to answer the foundational question of "What are we trying to protect against?"
3. The Framework Sub-Team will develop a model which applies a baseline set of requirements for all BES Cyber Systems which allows for enhanced requirements for:
    a. High impact
    b. Specifications for generation, transmission, and control centers
    c. Specifications for legacy vs. state-of-the-art equipment
    d. Connectivity considerations
4. The Framework Sub-Team will consider developing a framework for incorporating vulnerability assessments into the current standards for the purpose of allowing flexibility in applying security controls.

Following the discussion of the premises and prior to refining and finalizing the guidance statements, the SDT discussed the development of the framework. Some of those comments are noted below:

- **Manage security like reliability.** We need to manage our security posture the same way we continuously monitor the reliability of the grid.
- **Change the Zero-defect approach.** We have to change the "zero defect" approach to the enforcement of standards.
- Power to fix some of these in our hands, way to craft words. Requirements often written with zero defect approach. Maybe the real requirements- review every X month, fix. Can get us down the road fixing that.
- **Change the Industry approach to Self Reports.** We need to find ways to promote the feedback loop and self-correcting mechanism by giving rewards to detecting and fixing cyber security issues in a timely manner. We need to explore how we change current the self reporting syndrome. We could suggest adjusting the penalty range- automatically set at the floor if you have taken measures and self reported thereby starting at a lesser penalty.
- Look to other industries- e.g. FAA/pilots with anonymous database that can be reported and doesn't affect licensing.
- Jerry Cauley, President, NERC, has promoted a "lessons learned" process at NERC. NERC staff will look at all of the reports- incident, self, etc. and cull out lessons learned for the CIP.
- What kind of behavior do we want to incent? In the human resources area we "look monitor, find, fix and repeat."
- How do you cause good cyber security to occur?
- Self reports are not made public until they go to end of the enforcement process. CEII provisions protect details and names. Specific instances where self reports made public on CIP issues. NERC rules of procedures- protect details and identity.
- Remember everything that is public info- audit schedule is public information. Tenaska up for audit and include CIP.

- Model based on fear and politics. Entities deal with incoming from wall street, congress etc.
- Other problem with shielding self reports- industry gets no lessons learned for the industry. Information is shielded. Prevents this.
- **Uniformity of Audits.** We need to separate myths from facts and talk with the NERC audit people and test our assumptions.
- Address the issue of non-uniformity of audits across the region. When self reporting you could declare how you are fixing the issue to the region without it getting publicly reported, and go through a process of mitigation. Early cycle of correction in that method. Is something like that possible?
- This is a complex problem in that auditors are not uniformly sticking to the words in standards. Can the lack of consistency in application be fixed by CANs? May not be fixed by re-writing standards.
- **More granularity in standard writing-** access review list. Conduct a review, provide evidence you conducted a review. What are expectations? Won't go all the way in fixing a problem.
- Write programmatic requirements. Make a difference in how much effort. E.g. Requirement for training vs. awareness. Tracking training.
- Do we have a different set of requirements based on environment /equipment?
- Do we have multiple levels of requirements based on risk/impact (including communications)?

C. Organizing the CIP Format- Rember Round-Robin Perspectives on CIP Format

The Framework Team has been asked to provide a draft answer the question of the organization of the CIP going forward and has been developing a clearer documentation of the rationale for the changes reflected in the draft CIP 10 and 11. Following a question regarding guidance on the format by Dave Norton, the Chair asked each SDT member, through a round robin review, to describe their current thinking on the format for the CIP. He noted that at its Sacramento meeting the SDT was nearly evenly split on the format question. Several members noted they had changed their earlier position supporting the use the existing CIP 003-009 format and many now said that form should follow function and that either format approach, or even another format approach would be acceptable. The following summarizes the results of the round-robin review. Several members noted they were personally and not necessarily for their company:

- Those members open to creating a new standards format and not tweaking CIP 003-009 which could be a single CIP 11 or a sequence of separate standards (11,12,13, etc.) included: Rob Antonishen, Jackie Collett, Jon Stanford, Doug Johnson, Jay Cribb, Bill Winters, Bill Gross and Scott Rosenberger.

- Those members suggesting that form should follow function and were neutral on the format or could live with it either way consistent with the function, included: Tom Stevenson, Joe Doetzl, Kevin Sherlin, Dave Revill, Dave Norton Gerry Freese, John Lim, Phil Huff, Jeff Hoffman.

- Those favoring tweaking the existing 3-9 but may be willing to accept another formatting approach included: John Varnell.

- FERC representatives suggested the SDT focus on getting the requirements right and less on the format.

- Participants also offered perspectives on the changes and the format.

Stu Langton summarized the results of the exercise suggesting there was in evidence a lot more openness around this issue than in Sacramento and a shared value of getting the requirements right first and then organizing the format. The Framework Team could focus on the goal of eliminating or reducing cross-linking in the standard requirements and TFEs. The Chair suggested there was not a sense from the team for a basic shift in direction and asked the Framework Team to continue its efforts in preparing a strawman for the December, 2010 meeting in Orlando. He also noted that the communication plan for industry outreach and education that the Team is developing will be critical to the success of the SDT.

IV. NEXT STEPS AND ASSIGNMENTS

The Team reviewed the steps and assignments coming into the Baltimore meeting. The SDT agreed to engage in a series of conference call meetings (Monday-Friday, 11:00 a.m.-3:00 p.m.) the week before the Baltimore meeting to review industry comments and review and refine a set of strawman SDT responses to the comments. Howard Gugel will develop and circulate an initial strawman of responses to the industry comments drawing on the webinar responses reviewed in Toronto.

Tom Stevenson provided an overview of Constellation Energy's facility in Baltimore where the SDT will meet in November.

The Chair thanked Rob Antonishen for his excellent hosting of the SDT in Toronto.

The meeting adjourned at 4:40 on Thursday

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 EDT
Draft 27th Meeting Agenda
October 12, 2010, Tuesday- 8:00 AM to 6:00 PM EDT
October 13, 2010 Wednesday- 8:00 AM to 6:00 PM EDT
October 14, 2010 Thursday- 8:00 AM to 6:00 PM EDT
Toronto, Canada

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

Proposed Meeting Objectives/Outcomes:

- To review September 29 webinar questions and begin the development of a response document for industry posting
- To review and discuss and test acceptability of proposals for addressing key issues presented by the CIP Framework Team
- To review the Sub-team summaries of the CIP 010 & 011 and Workshop industry comments and discuss possible responses in light of the framework review
- To agree on next steps and assignments

Tuesday, October 12, 2010 8:00 a.m. - 6:00 p.m. EDT
- Introduction, welcome -*(Morning)*
- Receive updates on other related cyber security initiatives- *NERC Staff and SDT Members (Morning)*
- Review meeting and milestone schedule for CIP 002-4 and CIP 010 and 011 *(Morning)*
- Review changes to CIP Version 4 prior to ballot (CIP-002-4 R3 and CIP-008-4 applicability)
- Review results of September 29 CIP 002-4 Webinar *(Morning)*
- Participate in ERC Event Process Analysis Webinar and discuss implications for CIP development
- Draft responses and consider any changes to CIP-002-4 based on September 29 webinar questions *(Afternoon)*

Wednesday, October 13, 2010 8:00 a.m. - 6:00 p.m. EDT
- Receive a report from the team assigned to work on the framework *(Morning)*
- Discussion of Framework Team key issues *(Morning)*
- Review and provide feedback on the acceptability of the presented approach *(Afternoon)*

Thursday, October 14, 2010, 8:00 a.m. - 6:00 p.m. EDT
- Continue discussion of prospective framework *(Morning)*
- Review Sub-teams summaries of industry and Dallas workshop comments on CIP 010 & 011
- Discuss potential responses in light of the framework
- Review Preparation for CIP 002-4 Team Organization for Responding to Industry Comments before and in Baltimore *(Afternoon)*
- Review SDT November, 2010 Baltimore Meeting Agenda (*Afternoon)*

Appendix # 2 Attendees List
October 12-14, 2010 Winnipeg

Attending in Person — SDT Members and Staff

1. Rob Antonishen	Ontario Power Generation
2. Jackie Collett	Manitoba Hydro
3. Jay S. Cribb	Southern Company Services
4.Gerald S. Freese	America Electric Pwr.
5. Jeff Hoffman	U.S. Bureau of Reclamation, Denver
6. Doug Johnson	Exelon Corporation – Commonwealth Edison
7. John Lim, Chair	Consolidated Edison Co. NY
8. David Norton	Entergy
9. David S. Revill	Georgia Transmission Corporation
10. Jonathan Stanford	Bonneville Power Administration
11. Tom Stevenson	Constellation
12. John D. Varnell	Technology Director, Tenaska Power Services Co. (W/Th)
13 William Winters	Arizona Public Service, Inc.

SDT Members Attending via ReadyTalk and Phone

14. Joe Doetzl	Kansas City Pwr. & Light Co
15.Sharon Edwards	Duke Energy
16. William Gross	Nuclear Energy Institute
17. Phillip Huff, Vice Chair	Arkansas Electric Coop Corporation (W/Th)
Rich Kinas	Orlando Utilities Commission (Tu/W)
18. Scott Rosenberger	Luminant Energy
19. Kevin Sherlin	Sacramento Municipal Utility District (Tu/W)
Scott Mix	*NERC*
Howard Gugel	*NERC*
Roger Lampila	*NERC*
Robert Jones	*FSU/FCRC Consensus Center*
Stuart Langton	*FSU/FCRC Consensus Center*

SDT Members Not Participating

Jim Brenton	ERCOT
Patricio Leon	Southern California Edison
Keith Stouffer	National Institute of Standards & Technology
John Van Boxtel	WECC

Others Attending in Person

Jan Bargen	FERC
Robert Preston Lloyd	Southern California Edison
Tom Alrich	Matrikon
Jim Fletcher	American Electric Power
Brian Newell	American Electric Power
Mark Simon	Encari
Jason Marshall	Midwest ISO
Roger Fradenburgh	NetSecTech

Others Attending via Readytalk and Phone
October 12, 2010, Tuesday

Wang, Anna	amwang@burnsmcd.com
le, vincent	vincent.le@ferc.gov
Hammad, Amir	amir.hammad@constellation.com
Wilson, Bryn	wilsonwb@oge.com
Rayo, Ingrid	ingrid.rayo@constellation.com
Kelly, Justin	Justin.Kelly@ferc.gov
Farquharson, Jerome	jfarquharson@burnsmcd.com
Hardiman, Rod	rchardim@southernco.com

October 13, 2010, Wednesday

Hardiman, Rod	rchardim@southernco.com
le, vincent	vincent.le@ferc.gov
Farquharson, Jerome	jfarquharson@burnsmcd.com
Wilson, Bryn	wilsonwb@oge.com
Kelly, Justin	Justin.Kelly@ferc.gov

October 14, 2010, Thursday

Name	Email
Rayo, Ingrid	ingrid.rayo@constellation.com
Wilson, Bryn	wilsonwb@oge.com
le, vincent	vincent.le@ferc.gov
Hardiman, Rod	rchardim@southernco.com
lopez, andres	andres.lopez@usace.army.mil
Hammad, Amir	amir.hammad@constellation.com

Appendix #3 NERC Antitrust Compliance Guidelines

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

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

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

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

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

Appendix #4
Review and Discussion of Results of September 29,2010 CIP 002-4 Webinar

The SDT reviewed, discussed and reached agreement on the over 100 questions and the actual responses provided during the webinar. Webinar questions were offered verbally and by a chat function. Howard Gugel noted that the final question and response document will be posted for industry review on the NERC website as soon as the SDT reviewed and agreed with the responses. The SDT agreed to craft, where needed, additional clarification comments to the member responses offered during the Webinar.

1. **What are reasonable costs? Slide 10**

   Comments on Response
   - Alan Mosher presentation of context and response. Slide speaks to "reasonable" costs.
   - Generally speaking we should de personalize SDT responses but not this one since Alan is not speaking for the SDT but for the Standards Committee.

   Final Response: (Allen Mosher) The idea here is that we all are subject to our budget constraints. We want to use our resources effectively. The question is, can we craft controls that present reasonable costs to the industry to secure BES assets from cyber attacks, and what's the best use of the resources? We could spend a lot of money getting perfection in one area, but since we're trying to accomplish defense in depth, we need to have controls that are balanced across all the requirements so that in total we get an effective Cyber Security program. So there's a balance in both the cost of requirements and, in my mind, across this whole reliability budget that each utility and the industry faces.

2. **Was the fact that the Second Ballot overlaps the Thanksgiving Holiday discussed? This only gives 5 business days for the industry to respond.**

   Response Comments, Tuesday
   - OK with response. A participant pointed out this could mean the SDT may get less industry response and review.

   Final Response: Yes. Unfortunately, that's just the way the timing fell, and in order for us to prepare this as a filing to FERC by the end of the year, that's just an unfortunate part of the schedule.

3. **Slide 14: Is the plan in addressing the remaining 50 FERC directives still to keep the CIP-003 through CIP-009 nomenclature or will it be to combine into CIP-011?**

Response Comments, Tuesday

- Edit the redundant response. OK

Final Response: We received a lot of feedback on whether to keep CIP-10 and -11 and CIP-3 through -9 from the informal comment period. We're still dealing with that as a Drafting Team and trying to determine the best approach to present those requirements. What we come forward with in July of next year will reflect where we're going as a team.

4. **Slide 17: Will the data request results be provided external to the SDT (e.g. industry, FERC, others)?**

Response Comments, Tuesday

- Make this a NERC response to the data request. Howard made edits.

*Final Response: "*Yes, they will be posted by NERC at some point. NERC is in the process of scrubbing the responses and determining how to post a summary But certainly, the results of that would have to be provided to FERC and to the participants. Individual responses will not be posted publicly, so that any individual entity cannot be identified."

5. **What is the process to update the criteria in the future? will it go through industry voting? Is there something in the NERC ROP to accommodate this?**

Response Comments, Tuesday

- Delete 2nd line of draft response.

*Final Response: "*Attachment 1 is part of CIP standard 002-4. Any changes to the criteria will have to go through the Standard Development Process*."*

6. **Does the definition on slide 19 apply to the StruxNet LNK Recommendation? Do you expect entities to report on DCS or SCADA that are not critical to BES?**

Response Comments, Tuesday

- Critical Cyber Asset Identification Slide 19
- Answer to first quest is No.
- This is an alert to industry and has nothing to do with the CIP standards.
- This is a NERC Rules of Procedures alert process.

Final Response: (Scott Mix) The Stuxnet alert advisory came out independent of any Standards or compliance or auditing actions, and so anything that happens in the Standards world is not directly applicable to the alerts that come out. Stuxnet was a mandatory recommendation with a required response. And as such, it actually falls

under the NERC Rules of Procedure, not the compliance program or in response to a Standards action.
***Additional clarification from SDT*:** The answer to the first question is No. The answer to the second question is Yes.

7. **Slide 16 - If the intent is to replace the non-uniform risk based methodologies with the bright-line criteria in new attachment 1, why does the new R3 still require Sr Manager approval of the risk based methodology as shown in Draft 1 dated 9/20/2010? It seems that Sr. Manager approval of the CA and CCA lists would be sufficient.**

   Response Comments, Tuesday
   - Howard Gugel will make the changes regarding the errata
   - Is there a fiduciary level manager sign off?

   Final Response: (Howard Gugel) "This was an oversight, and at the time when the Standards will be balloted, we will be issuing an errata change to R3 to remove the reference to the approval of the risk based methodology. There is one other area that was missed in the editing process (CIP-008-4). These changes will be made before the balloting is performed and the ballot body will be notified of the changes."

8. **Second question - How can compliance be measured for "anything else the RE wants to include"? This kind if ambiguity is not appropriate in a Standard.**

   Response Comments- Tuesday
   - "Any asset as a critical"

   Final Response: "This particular criterion is not intended to be measurable; it is an option that allows a responsible entity to identify any asset as a Critical Asset, it can be anything the entity wants to include. So from the point of view of enforcement, there's really not much in terms of how you measure that. However, any Critical Asset that you include in that list would also have to be evaluated to determine if it has identified Critical Cyber Assets associated with it."

9. **What is "bright-lines"**

   Response Comments- Tuesday
   - 1500 does not apply to blackstart?
   - Reference to 1.1.?
   - There are other criteria that apply.

   Final Response: Generally, bright lines are those types of criteria that have a very well defined threshold that allows you to decide whether a BES Asset is qualified as a Critical Asset or not. There are usually very definite numeric values which are not subject to any kind of evaluation or subject to engineering studies and such.
   For example, Criterion 1.1 refers to aggregate generation at a single location of 1,500 megawatts. This is a bright line. So aggregate generation below 1,500 megawatts does

not have to be identified as a Critical Asset based on Criterion 1.1, and aggregate generation that is equal to or above 1500 megawatts has to be identified as a Critical Asset based on Criterion 1.1.

10. Slide 22- How was the 1500 MW criteria determined and or what was it based on?

Response Comments- Tuesday

- 1/3 generation would be captured. Average of a sampling
- Average of the sampling of the reserve sharing. Missing WECC.
- Argument for average is weak.
- Chose number because 1/3 of generation fell into that. Took an average of those numbers.
- "Desk survey"- informal-
- "Determined" – vs. supported
- Additional clarification statement agreed to. U.S. Energy Administration source of the data-base.

*Final Response: "*In prior versions we had wording about reserve sharing, and that was the threshold to be compared for critical threshold for generation. We got a lot of feedback that that wording was confusing, that the amount referred to in the reserve sharing was not a specific amount, and that the amounts changed daily.
So we did an informal survey of the regions, and we identified what the megawatt value of the reserve sharing would be for various groups, and then we took an average of those numerical values. And that 1,500 megawatts represents that numerical average of the values of the reserve sharing amounts."
Additional clarification from SDT: The 1500 MW level was supported by looking at the DOE Energy Information Administration database, and it was determined that approximately a third of the generation in the US would be classified as Critical Assets.

11. Slide 22: Will nuclear units under the 1500 MW units be classified as critical?

Response Comments- Tuesday

- "Units"- Wording in standard- reference aggregate generation at a single plant location.

Final Response: "The standard as it stands today does not specifically call out anything special about nuclear units. You apply the same criteria that are in Attachment 1 that apply to generation and determine whether these are Critical Assets or not.
Additional clarification from SDT: The wording of Criterion 1.1 refers to aggregate generation at a single plant location, not unit specific.

12. Slide 22 - I assume critical assets "designated" by Transmission Planners will be independently verified?

Final Response: "According to our understanding of the audit process, pre work that would be done by the audit team in preparation for doing an audit against the revised CIP 002-4 would be to contact the appropriate transmission planners and planning authorities to determine if there were any assets that had been designated and verify that those assets were included in the Critical Asset list. That is consistent with the way other Standards that have linkages between them are audited."

13. **Slide 21: If existing Critical Assets do not meet the bright line criteria and are not identified under the catch all, what would the effective date of retiring them as Critical Assets? Would the implementation plan address this or would they drop off the list when CIP-002-4 becomes effective?**

Response Comments- Tuesday

- 3-6 years. Is this longer than the standard requires.
- "May" be retired? Keeps open the CIP 010-11.
- Scott checked with Roger and approved the language with edits.

Response Comments- Wednesday

- Joe Doetzl offered draft language. "The post version 4 version 4 standards…..
- OK with new language.

Final Response. "The implementation plan for the Version 4 CIP Standards does not specifically address this scenario, but since the methodology that identified them as Critical Assets is only required under Version 3 of the Standards, they would be retired as Critical Assets upon the effective date of the Version 4 Standards, which is when you're required to be in compliance with the new version of CIP 002-4.
The post version 4 standards are still in development and may impact your decision to remove assets from the list. So even though it may be retired as a Critical Asset, it still may be included as either a medium impact or a low impact in the future.
From a compliance standpoint, the compliance scope is either three or six years, so you would need to maintain any evidence of compliance for that asset during the time that it was on the Critical Asset list."

14. **Are we to understand that reliability purpose in 1.3 is for long term only (RMR)?**

Response Comments- Tuesday

- We didn't answer during the webinar? Spoke about RMR. (on row 45 -answer provided is right. Reference: See line 45).

*Final Response: "*See answer to question 44. (line 45)"

15. **Does this include black start even if it is the 3rd or 4th path**

Response Comments- Tuesday

- Question is confusing. Talking about a unit in blackstart.

- Are we talking about path?
- Path is dealing with cranking path not black start unit.
- Does blackstart definition include units and paths? This is adequately answered.

Final Response: What we've done in the attachment is use the term "Blackstart Resource," which is a term that is defined in the NERC glossary. As the Standard is currently written, if it's identified as a Blackstart Resource, it would be included as a Critical Asset, regardless of whether it's the third or fourth path. If it's in the Transmission Operator's restoration plan, then it is a Critical Asset.

16. **Slide 22 Can we discuss the definition of Plants with group of units? (16)**

Response Comments- Tuesday

- OK

Final Response: "This is in reference to Criterion 1.1, which says, "Each group of generating units, including nuclear generation, at a single plant location." This is generally understood to be a single plant, whether it's a single unit or all the units in that plant. One thing to note is that "plant" is not a NERC-defined term, so we can't really refer to "plant" as a defined term within the Standards."

17. **Slide #24 In the Rational document, page 15, the following statement is made: "While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets". This statement not based on any Commission approved Standard and goes could be interpreted as an unjust interpretation. Recommend a qualification of a MW level be added to 1.14, as written in CIP-010. If not all BAs, TOP's and RC's regardless of size will automatically be designated as a Critical Asset.**

Response Comments- Tuesday

- OK

Final Response: "As discussed in the Reference Document, this requirement is sourced from EOP-008. Control centers performing these functional obligations are considered important enough to require mandatory backup requirements and warrant designation as Critical Assets."

18. **Assume that a power plant has four 400 MW units and is > 1500 MW power plant and therefore meets the definition of a Critical Asset in accordance with attachment 1. Let's assume also that there are no systems (other than the EMS) that impact more than one of the four units. How would one go about determining if any DCS's or digital relays at the plant are critical cyber assets or not since in this example no cyber asset (besides EMS) can impact more than 400 MW? There seems to be a lack of bright lines specific to cyber assets within a power plant or substation.**

Response Comments- Tuesday

- Didn't respond to this in webinar.
- Proposed language: "only"? "excluding blackstart resources"
- "Only shared"?
- Is this "communications"? Adds a whole new layer.
- Need to evaluate before agreeing to the assumption about DSC or digital relays not impacting more than 400 MW?
- Lack of bright lines for cyber assets.
- Bright lines focus was for critical assets not critical cyber assets.

Final Response: Requirement R2 states "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes." The focus of Version 4 was to provide bright lines for Critical Asset identification, not Critical Cyber Asset identification.

19. Please elaborate on the term functional obligations in 1.14

Response Comments- Tuesday

- Rewrote the response referencing functional obligations from the NERC functional model.

Final Response: "Functional obligations are determined from the NERC functional model. That term used here refers to the tasks those functional entities (e.g. RCs, BAs, and TOPs) perform, which is referred to in EOP-008."

20. Attachment 1, 1.15 A Black Start Unit should not by itself trigger a GOP Control Center as a Critical Asset - The Black Start Unit is under the TOP Control Center during Black Start conditions - not the GOP Control Center

Response Comments- Tuesday

- "Blackstart under" TOP?
- Verbal control from a GOP? Does the control center become a critical asset.
- Vulnerability in non black out condition.
- Disable it?
- Answers the question what has been posted.
- Is what has been posted what the SDT wants?
- Separate determination for a critical cyber asset?
- Is what the standard says what we intended?
- Are we reinforcing this?

Final Response: "As currently proposed, Criterion 1.15 states that each generation control center and backup control center used to control generation identified as Critical Assets, or used to control generation for an aggregate of 1,500 megawatts within a single Interconnection is a Critical Asset. So if a Black Start unit is designated as a Critical Asset and you have a control center that is used to control generation for that Critical Asset, then that generation control center is a Critical Asset."

21. Which guideline is being referred to?

Response Comments- Tuesday

- Several "guidance" references-all posted. Assume it is the "Guideline for identification for critical assets, etc"

Final Response: "The SDT notes that this is probably in reference to the difference between control centers and control rooms. This guidance can be found in *Security Guideline for the Electricity Sector: Identifying Critical Assets*, which can be found at http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdf . Additional guidance documents can be found on the NERC Reliability Standards page under Critical Infrastructure Protection (CIP)."

22. Can you clarify what is meant by "automatic load shedding"? Would this include load management systems that have the ability to reduce loads by greater than 300 MWs?

Response Comments- Tuesday

- This was the answer of the member at the time.
- What we have in the response is not entirely clear.
- "language"- offered- for clarification.

Final Response: "We had a somewhat extended discussion in the Drafting Team about the term "automatic", and in the paper that we put out, we discussed what we mean by "automatic." It includes those assets, those systems that are in the transmission system that would automatically trigger load shed under certain conditions. So those are certainly in scope here. As far as computer systems, the criteria says, "common control systems capable of performing automatic load shedding of 300 megawatts or more." So if you have a single control system that is capable of performing automatic load shedding of 300 megawatts or more, that is in scope.
Additional clarification by the SDT: If you feel that additional clarification on the definition is needed, please provide that in your comments along with a proposed solution.

23. Could you please expand on what is meant by Control Generation in 1.15 Criteria.

Response Comments- Tuesday

- Expand on what we mean by control?
- "by which generation can be controlled?
- Can ISO send a zero set point?
- Use "supervisory control?" What does this mean?
- If GOP supervises a plant-
- Further discussion needed
- Need to do this now.
- Review "control center" definition.
- "display of data" is not critical. Had trouble with several things in the definition. This is on another team.
- Functional obligations of the GOP? Instead of singling out control center. Control centers performing functional obligations of the GOP…..?
- Part of comment period.
- Putting this out for comment.
- What does control generation mean?
- Provide us alternative language as part of their comments. E.g. given.
- Little time to respond to comments and no comments. If we do a better job of answering.
- Primary objectives- get the responses finalized. Use this time to come up with solutions.
- Taking the time.
- Go through get out in front. Get what we can resolved now. Get through the response document
- We haven't answered what was asked for. What do we mean when we say control generation. Guideline re control center- 1st aspect of control center.
- Howard Gugel will work on language.
- Struggling without common terms. Answer the question with the SDT's intent. We may need others to define. Other cyber contexts- years of discussion allow for.
- The webinar response was not correct reading of the standard language.
- As a team what do we want to say. Reset the common intent and common definitions.
- Some others not responded.
- Can we say in this standard what the term means- e.g. for the purpose of this requirement or standards… Each one has to have those words.

Response Comments- Wednesday

- "Monitoring and control?"
- Question focuses on control generation. 1.15.
- Version 1 FAQ- monitoring and operating control functions- covers the water front.
- Control = Seeing their display- picking up phone and telling them to do something.

- Operator is part of completing the control loop.
- Operator is a "filter"-
- Monitoring data that would affect the operation- considered in scope of control of the critical asset.
- Why not include monitoring? Monitor for maintenance, for trade,
- What was meant was monitoring for control" Control of generation includes Monitoring control.
- "Display of data" as a term is problematic.
- 1.15 Refers only to "control centers"
- Only looking for those with supervisory or automated control. Only consider for 1.15.
- Not one bullet vs. 5 but a non-binding definition.
- It means what it meant in Version 3.
- "supervisory control" used in SCADA. Is this different?
- In terms of the guidance document- meant in terms of SCADA
- Functional model- "as directed by BA and TOP" GOP receives that direction and makes changes.
- Identify critical asset, later further define. RE would further investigate to see if they have critical cyber assets. Possibly brings in your cyber equipment. If doing it by voice.
- Puts you on a critical asset list.
- Purpose not to include monitoring was to not to include qualification.
- New language- on functional model.
- Delete the 2nd paragraph. OK.

Final Response: There are a number of generation control centers that really just monitor, and if you need to actually do generation control, they don't actually have the capability of doing that, and they would have to call up the actual local control room to be able to effect those controls. For these, the discussion was that these types of control centers are not really in scope unless they have the ability of actually controlling generation.

Additional clarification by the SDT: Based on the language in the functional model, a Generator Operator is responsible to adjust "real and reactive power as directed by the Balancing Authority and Transmission Operator." A control center that provides this functionality *would be considered a Critical Asset if it meets the rest of Criterion 1.15.)*

24. CIP-002-4 attachment 1, 1.15 includes control centers that control critical assets, in addition to the 1500MW criteria. You didn't mention that - has that changed?

Response Comments- Tuesday

- Linked to the ones above.

Final Response: No, these are required to be designated as Critical Assets as well

25. Question about Comment stated during Slide 24: "Generation Control Centers are those locations which perform control of more than one location, while Generation Control Rooms perform control for one location." I would like confirmation that a Control Room controlling multiple Units, at the same location and fenced perimeter, is still considered a Generation Control Room, and not a Control Center.

Response Comments- Tuesday

- Good as is.

*Final Response: "*That is correct. We are targeting those that are controlling multiple generation locations. There is some discussion of that in the guideline for identification of Critical Assets for CIP Version 1 and 2. There is a discussion of control room and control center there, and this is what we mean by a control center in this criterion."

26. You need to provide guidance on control centers. There are some TOPs that operate only low voltage transmission. 46 kV, 69 kV and 115 kV are examples. None of these facilities qualify as Critical Assets from a transmission perspective. These facilities are often operated and monitored from a dispatch center using SCADA. Would the current CIP-002-004 language define these dispatch offices as "Control Centers?" Is there some NERC document that defines these dispatch offices as something other than a control center?

Response Comments- Tuesday

- Ok
- If you have a control center 115 KV but has load shedding capability, put that entire control center under scope.
- Criteria speaks to control systems.

Final Response: The NERC Guideline on Critical Asset Identification has a good discussion of Control Centers. For the purpose of the this standard, control centers that perform the functional obligations of Reliability Coordinators, Balancing Authorities or Transmission Operator are designated as Critical Assets. For generation, part 1.15 of Attachment 1 designates generation control centers that control generation for Critical Assets or that control generation for 1500 MW or more in a single Interconnection as Critical Assets.

27. How would the implementation plan address where we have a currently identified CA, but based on recently issued guidance, have now identified new CCA's in the CA?? Do we have 18 months to get the new identified CCA's into compliance?

Response Comments- Tuesday

- Ok

Final Response: "The assumption is that the question is referring to the guideline for identifying Critical Cyber Assets that was approved by the NERC Critical Infrastructure Protection Committee back in June. Specifically, we have not introduced additional language in the implementation plan to address this situation. Because we did not actually modify the way that Critical Cyber Assets were identified in Version 4, this situation is handled for Version 4 the way it would be handled in Version 3 in that an entity would need to refer to the Implementation Plan For Newly Identified Critical Cyber Assets and Newly registered Entities to determine the appropriate milestone that that plan identifies."

28. Slide 22: EOP-005-2 is not yet mandatory. Does the associated Blackstart definition only impact version 4 of the CIP standards (i.e. CIP-002-4)?

Response Comments- Tuesday
- OK

Final Response: The definition of Blackstart Resource was approved by the NERC Board of Trustees effective August 5, 2010.

29. On slide 38, it was noted that the key words were "support and maintenance". If those words are so key, how come they don't appear in the language of the requirements within the UASAR?

Response Comments- Tuesday
- Ok
- Doesn't occur in the SAR. In the revision history. Support and maintenance not mentioned. Its in the standard and in the SAR.

Final Response: has been communicated to the UASAR drafting team for consideration.

30. For Jim Brenton - slide 39 - is this the draft document that is posted on the project page? If so, how does the document move from the "draft" version to the "final" version?

Response Comments- Tuesday
- Will work with Jim.

Final Response: This document is posted on the Project 2010-15 web page. This document will be considered final upon approval of CIP-005-4. Until then, the document will continue to be modified based on comments received by the Project 2010-15 Drafting Team.

31. Will you be providing links to the documents mentioned in numerous slides i.e. slide 39 CIP-005 guidance document

Response Comments- Tuesday
- Ok

Final Response: They are posted at: http://www.nerc.com/filez/standards/SAR-Urgent_Action_Revisions%20to%20CIP-005-3.htm

32. When will the redline versions of the changes to CIP003-CIP009 be made availale to the industry?

Response Comments- Tuesday
- Ok

Final Response: They have been posted in the Project 2008-06 Phase II project page. http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html

33. Slide 22 - How is "initial plant for restoration" defined?

Response Comments- Tuesday
- Answer does say how it is defined. Did this come from EOP 005-2. “Initial plan for restoration.” Not defined as glossary term.
- Not defined. Is in an old standard.
- Misquoted on a slide- standard doesn’t use.
- Howard Gugel will draft new language

Final Response. The criterion calls for the term "Blackstart Resource," and as long as the facility is identified in the Transmission Operator's restoration plan as a Blackstart Resource, then it should be designated as a Critical Asset.
Additional Clarification from the SDT - initial plant for restoration is not a defined term. The slide was an attempt to frame a discussion around Blackstart Resources, specifically concerning initial switching requirements.

34. Please clarify when CCA is replaced by H/M/L?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

35. There is no more CIP-10 AND CIP-11?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

36. Has the drafting committee abandoned the H,M,L categorization method?

Response Comments- Tuesday
- Ok

Final Response: The post version 4 standards are still in development.

37. Regarding CIP 002 Attachment 1, 1.1. can you define the word capability

Response Comments- Tuesday
- Ok
- Howard Gugel has language: "the drafting team referred to MOD-024-1 when developing 1.1. Please refer to this standard when determining net Real Power capability.

Final Response: The drafting team referred to MOD-024-1 when developing Criterion 1.1. Please refer to this standard when determining net Real Power capability.

38. CIP 002-4 R3 includes verbiage for annual review of risk-based methodology

Response Comments- Tuesday
- The answer is yes.
- Already answered in question 6.

Final Response: Refer to answer for question 7 (line 8)

39. What version of the CIP standards are going to be audited against, version 1, 2, or 3?

Response Comments- Tuesday
- Audit for time frame based on which version enforced.
- Version 3- does not begin until January 15 2011.

Final Response: The answer is yes. It depends on the specific timeframe that the audit is addressing. Remember that the audits look back three years or six years, depending on the type of entity that you are, and you are expected to demonstrate compliance with the Standard that was in force at the time of the audit. So right now, if an entity is being audited today, as we speak, they would be expected to demonstrate compliance with Version 2 of the Standards going back to April 1, and Version 1 of the Standards going before April 1. After this week, next week, they would be required to demonstrate compliance with Version 3 for anything going back to October 1, Version 2 going back to April 1, and Version 1 moving back beyond that.

Assuming that the implementation timeframe for Version 4 comes in within the general timelines that were discussed in the presentation, it is possible that the three-year look-back period will have requirements that will have the expectation that you would have to demonstrate compliance for all four versions of the Standards, depending on which particular timeframe the auditors are looking at. And any further information on that, you would have to discuss with your particular audit team to determine exactly how they're going to request that kind of evidence and what they're going to be looking for.

40. How "robust" are the 1500 MWe and 15 minute limits in R1 Attachment for Generators, i.e. voting position may depend on these limits.

Response Comments- Tuesday
- The limit is what it is.
- Proposed limits. You are encouraged to submit comments.
- It is a politically motivated number addressing concern. Can't rationalize any number.
- Refer to question 10 (line 11)

Final Response: Please refer to the answer to question 10 (line 11).

41. Is it still acceptable to have critical assets with no CCA'a

Response Comments- Tuesday
- Use Howard Gugel's language-.

Final Response: "It is not necessary for a Critical Asset to have Critical Cyber Assets."

42. Question - It appears that NERC has addressed a common way to determine Critical Assets, but NERC did not define "essential to reliable operation of a Critical Asset" thus, the new CIP-002-4 standard does not seem to actual compell the Industry to protect any more devices.

Response Comments- Tuesday
- Issues of identifying critical assets"
- The point of standard to identify critical cyber assets.

Final Response: 'The scope of the changes to CIP-002−4 is directed at resolving a certain number of issues of identifying Critical Assets.'

43. Question regarding control centers at the distribution side with automatic load shed capability of 100MW or more. Will these be expected to be evaluated under CIP 002-4?

Response Comments- Tuesday
- Flag to come back to.

Final Response: Currently the criteria says that you have to designate as Critical Assets those systems that are capable of load shedding automatically--automatically load shed--300 megawatts or more within 15 minutes.

***Additional clarification from the SDT*:** Please refer to the answer to question 22.

44. You mention required to run for reliability is not the same as RMR. Is the guidance to then simply request a determination from the Trans Planner?

Response Comments- Tuesday
- Tie to automatic load shed.
- OK. With edits.

*Final Response: "*The responsible entity has to check with his Planning Coordinator or Transmission Planner on whether his unit is designated, or what other units are designated as "must run for reliability reasons." In certain regions, the term "RMR" is used for different reasons."

45. Could you post or advise on the specific URL where CIP info is included?

Response Comments- Tuesday
- OK.

Final Response: They have been posted in the Project 2008-06 Phase II project page. http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html.

46. Will there be a formal comments period and ballot available for the changes being introduced for CIP003-CIP009?

Response Comments- Tuesday
- OK.

Final Response: The conforming changes to CIP-003-CIP-009 have been posted. The comment period and ballot are coincident with the CIP-002-4 standard.

47. Why wasn't "essential to reliable operation" addressed?

Response Comments- Tuesday
- OK.

Final Response: This is part of the definition for Critical Cyber Asset. The definition was not changed. Version 4 is narrowly scoped to address issues with Critical Assets.

48. Has FERC reviewed the proposed implementation schedules and are they in agreement?

Response Comments- Tuesday
- OK.

*Final Response: "*FERC approved the Version 3 Implementation Plans. The Implementation Plan for Version 4 will be submitted for FERC approval with Version 4 of the CIP standards."

49. If the revised CIP-005 refers to "guidelines" what is the risk that a utility interprets "guidelines" as optional and an auditor doesn't?

Response Comments- Tuesday
- CIP 005 doesn't refer to guidelines. No standard refers to guidelines.
- The auditor works to the requirements not the guidelines.

*Final Response: "*There is not a reference to a "guideline" in CIP-005-4. The auditor audits to the standards/requirements, not any guidelines."

50. In relation to R2.1, is there any intention to remove the serial exemption in the future? Previous draft version 4's have removed the serial exemption. Is this intended to be reintroduced into future revisions of the standard?

Response Comments- Tuesday
- OK.

*Final Response: "*The connectivity qualifications for Critical Cyber Assets still apply in CIP-002-4. Post Version 4 development is in progress, and connectivity is a consideration in the application of security controls."

51. Please provide additional clarification regarding the black start and cranking path brightliness associated with CIP-002 V4.

Response Comments- Tuesday
- Initial switching requirements and multiple path options are used in criteria?
- Lack of clarity comes from the sourced standards..
- Referring to the Transmission Operators restoration plan?
- What does multiple path mean?
- Is it the first load that you sync to?
- This was debated right before we posted.
- Is there a standard way of testing black start capability? Following the EOP? Testing the unit.
- Reference those are out of the EEI. Wording added. Consider including examples in guidance document.
- Jackie Collett and Doug Johnson will look at wording at what in standard. Address that language which isn't clear.

Response Comments-Wednesday
- Wish there was something about EOP.
- The SDT moved away from using the term "cranking path" because it wasn't defined.
- The proposed response language is consistent with what we have in the draft standard.

- EOP 005-2 requires testing everything in your plan for 3 years. Whatever you tested is critical, not what you have in the plan.
- "The choice of the next load" is key?
- First part of change reference cyber assets. Take the first reference out.

*Final Response: "*The intent of Criterion of 1.5 is to identify enough Cranking Path Facilities required during initial restoration as Critical Assets, up to the point where the entity has a choice of the next Facility or Facilities to use as part of the Cranking Path. The result is to provide protection for the constrained portions of the Cranking Paths, and to allow an entity some flexibility in defining their restoration sequence during an actual event."

52. Where can I find a document that summarizes only the differences between Rev 3 and the proposed 4?

Response Comments- Tuesday

- OK.

Final Response: The redline versions provide changes from Version 3 to Version 4. The mapping document also provides a review of changes.

53. Slide 16 - please explain the term "significantly mitigate" as it relates to oversight

Response Comments- Tuesday

- OK.

Final Response: The FERC directive really applies with respect to the previous Versions 1, 2, and 3 Standards where entities were using their self-defined risk-based assessment methodology to define Critical Assets. Paragraph 439 of Order 706 basically talked about the requirement for some oversight over that list of Critical Assets to ensure that it is adequate or not.
The opinion of the Drafting Team with respect to this particular directive from FERC is that by the use of bright line criteria in Attachment 1, there is no longer a need to verify the list, because it is a list derived from bright lines. A BES asset is either in or out, or the criteria are bright enough so that you can determine whether the Critical Asset qualifies or not, so there is no longer a need for oversight. "Significantly mitigated," means that, if not eliminated, there is significant mitigation of that requirement or of the issue by the use of bright line criteria.

54. For entities that have not claimed any CC's, 24 months could pose an extreme hardship both staffing and financially. Many entities have budgets that have been set for 2011 for both staffing levels and for finances. Could this implementation plan be expanded out to allow entities to plan financially and staffing wise?

Response Comments- Tuesday

- OK.

Final Response; The 24 month period to comply for entities who had not previously identified Critical Cyber Assets is the timeframe that's in the existing IPFNICCAANRE, or Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This is the currently approved implementation plan.

55. Item 1.6 on Attachment 1 of CIP-002-4 uses the term "Transmission Facilities". As defined in the NERC glossary this is a very broad definition covering lines, generators, shunt compensators, transformers, ETC. Facilities inside a substation enclosure can be protected but not miles of lines. Can you please clarify?

Response Comments- Tuesday

- Language okay substantively. Jackie will work with Howard for some editorial suggestions.

*Final Response; "*The standard does not require the protection of Critical Assets. It requires the protection of Critical Cyber Assets. So whether your cyber asset is in a centralized location within a substation, or a little away from the substation, that cyber asset would be subject to the requirements of the CIP Standards if it is essential to the operation of the Critical Asset."

56. Are isolated SCADA systems required to comply with these NERC reporting requirements

Response Comments- Tuesday

- Meet criteria for CAs and qualifications for CCAs?
- OK with Howard Gugel.

Final Response: Yes, if their associated BES asset meets the criteria for Critical Assets and the SCADA meets the qualifications for Critical Cyber Assets.

57. There are entities that have performed varies technical analysis to show that the requirements of attachment 1 do not affect the BES. Will these studies be considered to have an asset NOT defined a critical asset.

Response Comments- Tuesday

- Small coops- fall under this with possible expenses.
- Should we revisit this?
- Based on what we have out as CIP 002-4. They are critical asset if they meet.
- What is definition of a proper "authoritative study" to determine these and codify in the standard? Probably couldn't do.

- If we open any criteria up to evaluation to allow an exception it will produce a new "can of worms" and TFEs. Will this puts back on the table someone to review and approve a criteria?
- The ability to have custom user defined studies introduces the need for oversight which is what bright lines are trying to eliminate.

Final Response; No, if a BES Asset meets any of the criteria in Attachment 1, it must be designated as a Critical Asset. The ability to have user-defined technical analysis to exclude an asset that would meet the criteria of a Critical Asset would introduce the need for oversight, which defeats the purpose for bright line criteria.

58. What is meant by "single plant location" in criterion 1.1 of attachment 1? What about adjacent plants?

Response Comments- Tuesday

- We mean area encompasses a plant.
- We don't have the answer that what is a plant.
- Can a plant have multiple shipyards.
- Gerry Freese will draft a strawman response.

Final Response: Single plant location refers to a group of generating units occupying a defined physical footprint and designated as an individual "plant" using commonly accepted generating facility terminology. Adjacent plants would be defined using the same criteria. The units do not necessarily have to be connected to the BES at the same substation or interconnection point in order to be considered a single plant.

59. Was CAN-005 sent out via the NERC Alert system only?

Response Comments- Tuesday

- OK.

Final Response: No, CAN-005 was issued by compliance through a notice to NERC stakeholders.

60. Shouldn't the current CIP-005-3 have the same modifications as CIP-003 thru CIP-009 to prevent complications for Nuclear facilities?

Response Comments- Tuesday

- OK.
- Removed nuclear exclusion to be consistent with 706 B. Applied only to US jurisdictions not to Canadian facilities. Handled by CNSC.
- Not a conforming change, but an actual substantive change? No it is conforming.

Final Response: Conforming changes will be made upon filing.

61. Item 1.7 on Attachment 1 of CIP-002-4 was changed from "4 or more" to "3 or more". This has a tremendous impact on affected transmission facilities. Can you please explain the reasoning behind this change?

Response Comments- Tuesday
- Drafting team felt it was appropriate to refer to connected transmission substations to address parallel lines
- Not doing generating sub-stations.

Final Response: "In order to be more accurate in terms of the impact, the Drafting Team thought that it was more appropriate to refer to the number of connected transmission substations instead of lines connected to any particular transmission sub-station. The intent was to get away from the double-circuit conditions and to include facilities that are actually more a part of the network than simple substations with double circuits between them."

62. Will the regional entities push back if assets are removed from the CA lists because of the new criteria?

Response Comments- Tuesday
- SDT can't comment on this.

Final Response: The drafting team cannot comment on the possibility of push back.

63. Is the remote access Reference\Guidance document available yet?

Response Comments- Tuesday
- OK.

*Final Response: "*This document has been posted to the draft CIP-005-3 Modifications Urgent Action Standard page."

64. If the RE designates an entity as a CA, should the RE be responsible to communicate the determination or will the responsibility be on the entity to prove they were not designated as such for audit purposes?

Response Comments- Tuesday
- OK.

*Final Response: "*With the bright-line criteria, the responsible entity should be able to determine its own Critical Assets. Input from the RE or other registered entities may be required for that determination, in which case, the responsible entity is responsible for soliciting that information."

65. Will the Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets be updated and included with the approved Version 4 CIP Standards posting?

Response Comments- Tuesday
- Guideline doesn't need to be updated since haven't changed critical cyber asset.

*Final Response: "*The SDT will discuss necessary changes with CIPC, since they own this document."

66. A SCADA system is capable of opening breakers that would shed 300+ MWs of load but is not presently programmed to perform automatic load shed. The SCADA owner is not a BA, RC or TOP. Is the SCADA system a critical asset under 1.13 of CIP-002-4 attachment 1?

Final Response: Please refer to the answer to question 22.

67. Will it take a SAR to change the 1500 when needed

Comments
- OK.

Final Response: The criteria in attachment 1 are part of the CIP-002-4 standard and must follow standard revision procedures.

68. So since there is no technical justification for generation; what is the justification for the transmission thresholds?

Comments
- OK

Final Response: The reference document outlines the rationale for the criteria.

69. Would David Revill repeat his comment regarding Effective Date as determined by NERC- vs. FERC-approval?

Comments
- In Canada vs. U.S.? In the presentation.

Final Response: (from Speaker Notes) All entities should be compliant with CIP-002-4 on the Effective Date of the Standard. The Effective Date is defined in the Standard to be the first day of the third calendar quarter after applicable regulatory approvals. For those that do not have an applicable regulatory approval, the Effective Date is the first day of the third calendar quarter after the NERC Board of Trustees adoption. For those in the U.S., this is at least 6 months following FERC approval.

70. Does Attachment 1 criteria 1.4 apply to all blackstart resources in the restoration plan or is it limited to those associated with primary restoration paths. For example, if a restoration plan lists several alternate paths in addition to the primary restoration path, would the resources associated with the alternate paths be considered critical assets.

Comments
- "primary restoration path?"
- OK with response.

Final Response: The criterion calls for the term "Blackstart Resource," and as long as the facility is identified in the Transmission Operator's restoration plan as a Blackstart Resource, then it should be designated as a Critical Asset.

71. Slide 24 / CIP2 R4 Attachment 1 paragraph 1.14. All TOP Control Centers and Backup Control Centers are being classified as High risk CA's. This is independent of the criteria for determining the criticality of the substations that they control (paragraph 1.6 & 1.7). Why are ALL of these control centers being included as high risk CA's via the bright line criteria?

Comments
- OK

Final Response: EOP-008 specifically requires control centers that perform the obligations of the RC, BA or TOP to have backups. As such, these control centers and backup control centers must be designated as Critical Assets, irrespective of size.

72. What is the new timeline associated with the development of CIP-010 and CIP-011?

Comments
- OK

Final Response: Posting for formal comment and first ballot in July 2011 and filing to FERC by the end of 2011.

73. Bright Line criteria question. In the case of generation controlled/dispatched by a "Control Center" for wholesale power marketing purposes, how do you determine the 1500MW value? Would that be an aggregate of the regulation/dispatch limits (since the entire output cannot be controlled) or the aggregate output of all generation under control?

Comments
- EOP 5? Doesn't deal with control centers but with units?
- 1.15- rated net real power capability?

- FLAG- DJ.
- Goes with 24-

Response Comments Wed.

- We expect to use the aggregate higher rate real power
- The aggregate output of
- Use the aggregate of the same criteria as 1.1.
- The answer to the question is th
- If you deviate from 1.1 criteria, the value changes on the fly.
- Nothing for reliability for control? Plant controlled for economics part of reliability of the BES.
- If this control system tied to anyone else?
- 2 sentences.?
- Encourage more people to vote no with comments.
- "Part of the reason for this is that data flowing through the control center to others is the full output of the center."
- Does having the ability to take them off line do that.
- Multiple scenarios out- do we allow generation control centers to use the smaller number, and potentially lose some of those that are a data source. Or more fancy words to try to lock those in.
- Use the larger of the values. Use the same as 1.1. Our standard doesn't distinguish between marketing and reliability.
- Nameplate minimum and maximum loads are known.
- Switched off of nameplate because of the variability.
- Respond to what the standard is today.
- Say we are doing this on a generation basis. Wholesale market is not part of reliability. "
- The control center is identified because it is performing generation control irrespective of market purpose.
- We need to come back to this when we get comments on the standard.

Final Response: We would expect to use the same criteria as in Criterion 1.1. This is the aggregate output of all generation under dispatch/control. The control center is considered a Critical Asset due to the fact that it is performing generation control, irrespective of whether it is performing wholesale power marketing functions.

74. For determination of critical assets, how was the 1000 MVAR threshold for reactive resources arrived at?

Response Comments

- OK

Final Response: This value was determined to be reasonable by the CIP-002 subteam, based on generation criteria.

75. Why is there a preoccupation with moving to CIP 10 and 11? CIP-002 - CIP-009 have some natural breaks in them that can make them easier to administer among departments and the industry is comfortable with them. Why can't the team just continue to add new versions of the existing standard numbers?

Response Comments
- OK

Final Response: The drafting team continues to consider structuring options based on comments and requirements.

76. Attachment 1, 1.3 - can specific criteria be added to 1.3 for more specificity?

Response Comments
- OK

Final Response: Please propose alternative language that would clarify the criterion without introducing terms that already have implied use in certain regions.

77. **What about TFE's? RFC is requesting vendor letters, such as CISCO, that states that their product does not meet xxsx standard. This seems rather archaic. Can NERC make some sense of this issue?**

Response Comments
- OK

Final Response: The issue of Technical Feasibility Exceptions is high on the SDT's consideration in drafting the next version of the standards.

78. In the future, does the SDT still plan to revise CIP-002 to have all BES Assets identified as High , Medium, or Low?

Response Comments
- OK

Final Response: The SDT is still developing the next version. This is a consideration in this development.

79. As part of CIP-002-4 initiative, will there be a "bright line" categorization for Critical Cyber Assets?

Response Comments
- OK

Final Response: There is no substantive change in Version 4 for categorizing/ qualifying Critical Cyber Assets.

80. GO/GOP in some cases, such as wind generation, utilize remote operations centers operated by third party operators for tasks such as restarts and generation curtailments. What should be considered in determining if this is a Control Center as opposed to a control room?

Response Comments

- Point back to critical asset guideline for distinction between control centers and control rooms- perimeter around 1 or multiple locations. Point to same criteria. Point to Line 24
- This is pointing to a specific example.
- "Security Guidance for Electricity Sector: Guideline provides a discussion on the difference…..

Final Response: These are considered generation control centers subject to the criteria for generation control centers. The document "Security Guideline for the Electricity Sector: Identifying Critical Assets" provides a discussion on the difference between control centers and control rooms.

81. What if those group of units at one plant location do not all have common, interconnected cyber systems?

Response Comments

- Point to criteria in Attachment-
- Row 19 language.

Final Response: The plant location should be considered for qualification as a Critical Asset per Criterion 1.1. The cyber assets to be considered for qualification as Critical Cyber Assets have a specific qualification in R2 of CIP002-4, which is "For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes."

82. For Section 1.3 of CIP-002-4, shouldn't the SDT add that the PC or TP needs to notify the GO/GOP that his generation is designated as critical?

Response Comments

- OK

Final Response: The responsible entity has to check with his Planning Coordinator or Transmission Planner on whether his unit is designated, or what other units are designated as "must run for reliability reasons." Again, not all RMR are--in certain regions, the term "RMR" is also used for units designated as "must run" for market stabilization reasons.

83. When will the standards development and implementation plan be available on the NERC website?

Response Comments
- Current schedules were slides in the webinar.

Final Response: The slides for the webinar (including a high level view of the schedule) are available on the NERC site at http://www.nerc.com/files/CIP002-004-092910.pdf. The Implementation Plan for Version 4 is posted in the CIP Version 4 standards area.

84. If the effective date is the first day of the 3rd quarter after approval, couldn't the effective date be July 1 if FERC approves during the 1st quarter?

Response Comments
- Answer -No. assuming approval anytime during the first quarter,….

Final Response: No. Approval at any time during the first quarter would make April 1 the first day of the first quarter after approval, July 1 the first day of the second quarter after approval, and October 1st the first day of the third quarter after approval.

85. For example if an analysis has been performed at a local control center that opens all BES breakers and the BES remains stable would this study prevent the LCC from being a critical asset?

Response Comments
- Delete "for example"
- Line 58./ Question 57

Final Response: No, if the control center satisfies the criterion for control centers. Bright-lines do not consider the responsible entity's analysis or studies. Please refer to the answer to question 57 for additional clarification.

86. If the cranking path from Black Start resource to the next start resource is within the same substation, do you have to include the additional substations to the interconnecting/synchronizing point as critical assets?

Response Comments- Tuesday
- Is the answer yes or no?
- Blackstart unit in same substation?
- JC can look at this language differently. "Choice" is left open.
- More discussion on intent
- Look outside the sub-station?
- EOP 005, R15- have to have a plan and if all is covered..
- Flag this for further discussion.

- Glossary definition of "cranking path"? Could be within the same plant? The cranking path becomes a bus.
- 1.4 and 5 cover cranking path.

Response Comments- Wednesday

- If this substation has more than 1 path, then you could stop there.
- If meeting the EOP 005 standard, they will have additional paths.
- Draws picture. Straight bus with three transmission generators.
- Is this more than what the definition requires?
- Determines what is the unit to be started.
- If you are going to meet the other standards- says to the next generator?
- Good points. Issues with the GOP standards? NERC's definition of cranking paths?
- Wanted to use "primary cranking paths"- but it isn't defined. Was intended to be a compromise to scope this down. Did we go too far?
- Depends on what your restoration plan says.
- Hold this thought for revision of the standard.
- Interconnect is already in and this may already be covered.
- 1.10 covers this- Add 1.4 to 1.10.
- Concerns are valid but not in the CIP standards.
- 1.4 is needed to be added. The sub is part of the cranking path- where the generator connects to get it somewhere.
- Choices for path are units in the station. Take out first sentence?
- The GSU and a piece of the bus would be the cranking path in her example.
- Does it have to get of interconnecting to the system-
- Leave the one sentence

Final Response: It depends on how the Cranking Path is defined in the Transmission Operator's restoration plan.

87. Attachment 1, 1.8 - Facilities whose loss can create IROL's varies in time depending on what other transmission facilities are in service? Under what conditions is this determination to be made - in the planning horizon or the operating horizon. Also, is 1.8 meant to assume the loss of an entire substation?

Response Comments- Tuesday

- This has fundamental issues with it. Loss of facility doesn't generally create an IROL. Will be getting comments on this.
- In the planning horizon or the operating horizon
- Impacts that happen are what we are focusing on. Plan for varying operating conditions that occur.
- Don't generally violate an IROL.
- Do you calculate IROL for loss of a substation?
- Document the contingency but not doing anything about.

- Class D is the floor? Does this relate to IROLs? Not necessarily. Impact of the contingency not what kind it is.

Final Response: The criterion applies to the planning horizon. Part 1.8 assumes the loss of any combination of facilities including the loss of the whole substation.

88. Attachment 1 now creates a uniform criteria for Critical Assets. Why was the original requirement for determining Critical Cyber Assets left as "essential to reliable operation" which will just create the same problems with uniformity and auditing we had previously with Critical Assets?

Response Comments

- This was John Van Boxtel's question.

Final Response: The scope of the changes to CIP-002–4 is really directed at resolving a certain number of issues on Critical Assets.

89. 1. What devices are considered FACTS? 2. Is series cap considered a reactive resource? 3. Any IROL in Western Interconnection?

Response Comments

- SVCs, series caps,
- HVDC? Not
- #2? Yes. But may not always be a FACTS device.
- Where is definition of FACTS? Direct them there.
- WECC doesn't use the "IROL" philosophy.
- Language in Pittsburgh
- #3; FAC 014-2 requires all Reliability Coordinators to establish IROLs. Planning coordinator does the same thing.
- Refer to IEEE definition?
- Talk with planning coordinator and RC to determine if there are any in the region.
- SOL methodology.

Final Response: 1. IEEE has established a definition for FACTS. 2. Yes, but it may not always be a FACTS device. 3. FAC-014-2 requires all Reliability Coordinators and Planning Authorities to establish IROLs consistent with its SOL methodology. Please refer to your Planning Coordinator or Reliability Coordinator.

90. Are AMI systems considered to be ALS if they are 300mw or larger?

Response Comments

- Automated/Advanced Metering Infrastructure.
- Need to discuss the 300MW in the future.
- 300 MW- DOE requirement. Triggered a reporting.
- Doesn't stand up to the 1500 for generation.

- AMI distribution level? In scope? Either distribution provider. Load shed done at distribution level.
- Some could be inside commercial facility.
- Most load shed- done automatically.
- 300 MW is what it is now and get comments to change the number.

Response Comments- Wednesday

- Refer to question 22/response?
- Does the AMI act on its own?
- AMI issue before- "within 15 minutes" clarification.
- "Furthermore, the response time must be within 15 minutes in order to qualify.
- Functional model. DP implements under the direction of the TO.
- Should be the DP not the LSE in the CIP standard.
- Haven't decided yet included in DP moving forward.

Final Response: Please see the answer to question 22. Furthermore, the response time must be within 15 minutes in order to qualify.

91. Is there a specific implementation plan for CIP-005-4? Upon FERC approval, when would a Registered Entity be required to comply with the changes in CIP-005-4?

Response Comments

- 12-18 months- There will be an implementation plan developed and posted in next round of balloting.

Final Response: There will be an Implementation Plan for CIP-005-4, which will be developed and posted by Project 2010-15.

92. What is the meaning of "location" in 1.1 of Attachment 1 to CIP-002-4? For example: If a new 20 MW CT is located at an existing 1500+ MW plant and the CT connects to a different substation than the existing plant, is the 20 MW CT a critical asset?

Response Comments-Wednesday

- Refer to question.
- Plant is a critical asset by hypothesis. Unit is part of critical asset.
- Since the plant already meets bright line criteria, additional units installed at that plant….?
- If had a common control system.

Final Response: The plant would be considered a Critical Asset because it exceeds the 1500 MW threshold at a single plant location. For additional clarification in location, please refer to question 58.

93. Just as a comment, the redline and clean version of CIP-008-4 does not have the Nuclear plant exception removed. Will this be re-posted?

Response Comments
- OK. Have to go back to make sure proper language in for Canadian.
- Refer to question #7 and question on (nuclear)

Final Response: Yes, as part of an errata prior to balloting. Please refer to the answer to question 7 and question 60.

94. Where in the NERC Website that I can locate the presentation slides for today webinar?

Response Comments
- OK

Final Response: They are available at: http://www.nerc.com/files/CIP002-004-092910.pdf

95. Also, CIP-005-4 does not have the Nuclear plant exception removed either. Will this be removed with the next ballot of CIP-005-4?

Response Comments
- OK same as 93

Final Response: Yes, as part of an errata prior to balloting. Please refer to the answer to question 7 and question 60.

96. I don't believe the WECC has IROLs - how does this impact 1.8, 1.9, 1.12 in attachment 1

Response Comments
- If you have no IROLs in your area, in essence NO to 1.8,1.9 and 1.12. Copied from earlier response.

Final Response: FAC-014-2 requires all Reliability Coordinators and Planning Authorities to establish IROLs consistent with its SOL methodology. Please refer to your Planning Coordinator or Reliability Coordinator. If no IROLs have been designated, then an entity would have no assets determined to be Critical Assets based on Criteria 1.8, 1.9, and 1.12.

97. Is the 300MW load shed applicable if loads are connected less than 100kV?

Response Comments- Wed.
- **Refer to question 22.**

Final Response: No. This issue has been forwarded to Project 2010-15.

98. As it applies to the new NERC requirement in CIP005, will the term "remote access" be added to the glossary of terms?

Final Response: The definition is approved by the NERC BOT, and is provided in the current NERC Glossary of Terms.

~~**99. Are these slides currently posted on the NERC site and if so where are they located?**~~
- Asked and answered.

~~**100. CIP-002-4, R3 - includes verbiage for annual review of risk-based methodology - to be removed in errata?**~~

Response Comments
- OK

101. Since the EOP-005-2 standard and the Blackstart Resource definition are not yet FERC approved, how will this be coordinated with the FERC approval of CIP-002-4 which utilizes the Blackstart Resource definition.

Response Comments
- OK

Final Response: This issue has been referred to Project 2010-15.

102. For the purpose of interpretation of CIP-005-3, R6, does NERC consider this case as a remote access? "A person is using a CCA within an ESP to access another CCA in another ESP for the maintenance purpose."

Response Comments
- This issue has been forwarded to Project 2010-15.

Final Response: This issue has been referred to Project 2010-15.

103. Regarding the Control Room versus Control Center issue. Would a location that communicates with 2 substations, but controls a singular transmission asset be a Control Room or Center, whether the transmission asset is CA or not?

Response Comments

- OK

Final Response: It would be considered a control center if it is at a remote location.

104. Since it has been said that CIP-010 and 011 will eventually be implemented and CIP-010 (as currently drafted) CCA level impacts are High, Med and Low. If under CIP-002-4 bright line criteria in Attachment 1, you are not a CA, yet under CIP-010 you are implied to be a low impact CCA -- shouldn't there be a "no impact" category under CIP-010?

Response Comments

- Use the stock answer about future work part of CIP 010 and 11.

Final Response: The post version 4 standards are still in development.

Appendix #5 SDT Sub-Teams

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