

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

August 20, 2009 | 8 a.m.–5 p.m. PST
August 21, 2009 | 8 a.m.–4 p.m. PST
Charlotte, NC

SDT 706 August 20-21 Meeting Summary Contents	
Cover	1
Contents	2
Executive Summary	3
I. Introductions, Agenda Review and Review of SDT Work plan	8
II. Updates	9
A. Technical Feasibility Exception, NERC Rules of Procedure	9
1. Introduction.....	9
2. Review of Initial Proposals for Addressing TFE.....	9
3. TFE and Urgent Action Procedure Proposal	11
B. VSL/VRFs.....	14
C. Other Related Cyber Security Initiatives	14
III. CIP-002 Subgroup Reports	15
A. Overview	15
B. Subgroup Reports.....	16
1. Reliability Functions.....	16
2. List of BES Subsystems and/or BES Cyber Systems	18
3. BES Mapping.....	20
4. Cyber Analysis.....	23
5. Definition and Selection of Controls	28
VI. Next Steps and Closing	30
<i>Appendices Table of Contents</i>	<i>31</i>
<i>Appendix 1: Meeting Agenda</i>	<i>32</i>
<i>Appendix 2: Meeting Attendees List</i>	<i>34</i>
<i>Appendix 3: Meeting Evaluation Summary</i>	<i>36</i>

<i>Appendix 4: NERC Antitrust Guidelines</i>	<i>38</i>
<i>Appendix 5: SDT Work Plan Schedule</i>	<i>40</i>
<i>Appendix 6: TFE Matrix of Applicable Exceptions</i>	<i>43</i>

EXECUTIVE SUMMARY

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call (*See appendix #2*). The chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda (*See appendix #1*). The SDT adopted the July 13–14 meeting summary without comment or objection on Friday morning.

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

Vice Chair Kevin Perry announced, effective at end of October meeting, he will be stepping away from the SDT due to his responsibilities with his new job. He later suggested four principles to bear in mind as we develop the new standards requirements: remove variability; remove arbitrary decision making; criteria (requirements/controls) must be clearly understandable; and criteria performance must be auditable — the entity must be able to demonstrate compliance.

Mr. Langton reviewed the CIP-002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver and set up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the Chair and Vice Chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about four months to finish work of developing the CIP-002 draft to be released for industry comment in December 2009.

Jeri Domingo-Brewer briefed the SDT on the chair and vice chair’s presentation to the Standards Committee on a conference call earlier in August. The chair and vice chair agreed to provide the Committee with a “heads up” if there are any issues that might affect the SDT’s ability to get the job done in a timely fashion.

Kevin Perry and Scott Mix made the presentation on the development of the Technical Feasibility Exception process. Mr. Perry described the work of a NERC “Tiger Team” led by Mike Assante, NERC Chief Security Officer, with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Scott noted that the plan is to submit to NERC Board of Trustees for review and adoption at the October meeting following its consultation with the regional entity representatives. NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

On the first day the SDT discussed the current situation with the TFE process and whether the SDT should support efforts to find a standards solution approach to the challenge presented by TFE interim process in advance of the adoption of CIP Standards Version 3. Mr. Perry noted

that NERC's current view is that explicit or implicit "enabling language" references in the CIP standards will be required for an entity to request a TFE. Mr. Perry noted the current timelines associated with the NERC ROP.

Kevin Perry presented a proposal to the SDT to consider a relatively focused and narrow effort undertaken by a small team of SDT members to build upon the "Technical Feasibility Exceptions Matrix of Applicable Requirements" that he and others in the industry have been developing. It would propose a broader interim TFE process that will allow for a safe harbor for technical feasibility exceptions granted in the interim. An alternative presented by Gerry Freese would be to create a broader effort that would address the TFE and other interpretation issues raised by CIP Version 1 and Version 2. The SDT then identified the following pros and cons related to the proposals.

On day two, Mr. Perry noted he was withdrawing his proposal from day one and offered the following points for a new proposal in light of yesterday's discussion: The SDT should consider expressing support for the use of the NERC Urgent Action process to address the current TFE dilemma. This was done with the 1200 standard. He described the steps in the process and the SDT discussed the intent of the urgent action process and whether to adopt a resolution urging the Standards Committee to consider an urgent action approach. The facilitators noted this was an important issue and there seemed to be support for the SDT to help in some way to facilitate a solution.

After review of a possible resolution, the chair suggested instead that she draft a statement to the chair of the Standards Committee which should note that the SDT has identified an urgent challenge for the industry and that the Standards Committee should consider how to address the gaps that have been identified in terms of Version 2 of CIP standards and the proposed TFE procedure. The statement would note the SDT looked at trying to help with a solution given the skills, abilities and experience on the team, but the time needed would take away from the SDT's main charge and ability to complete the current work plan in a timely fashion. There could then be a summary of various options and implications in terms of the SDT work plan and the matrix attached. The team agreed by common consent that the chair should prepare and send a statement consistent with the spirit of the SDT's review and discussion.

Scott Mix reported on Dave Taylor's behalf that Version 1 is complete with a 92% quorum and 84% approval rate. This has been submitted to FERC on July 30. It will be adopted by FERC rule or by NOPR. Version 2 VSLs and VRFs is in the 30-day pre ballot review period. The expectation is for the second ballot to conclude in early October. NERC anticipates that FERC will take action on the CIP Version 2 standards in September/October 2009 as an Order or a NOPR. The SDT Webinar scheduled for next week was described by Phil Huff

The SDT reviewed the Subgroup process for developing CIP 002. Scott Mix noted that the SDT should begin focusing on both the content and format of a NERC standard and pointed to the possibility of a short set of clear requirements backed up by more detailed appendices or attachments.

CIP-002 Subgroup Reports presented their progress reports on day one and a follow up report on day two from their subgroup meetings.

Reliability Functions Subgroup leader John Varnell reviewed a draft list of assets the Subgroup was developing. He noted they haven't added any more functions but did combine some functions and expand on what was meant by each. He noted they hope to have a complete list by the end of the meeting. On day two he presented the following 9 functions noting each had a set of sub functions:

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

The List of BES Subsystems/BES Cyber systems Subgroup leader, Jay Cribbs presented an overview of the work done since the Vancouver meeting. Subgroup Leader Jackie Collett was on vacation but the group met once in the interim. He described the subgroup scope and expected output. He noted the subgroup has identified a list of issues and questions (“in this phase the subgroup is coming up with all questions and no answers”) that will guide their efforts to develop draft requirements. On day two he offered the following points:

1. We will not outline the process for “how” to create the lists. The white paper gives flexibility in the creation of the lists and allows entities to take a primarily cyber systems oriented view if they wish.
2. Assets and systems that are below the mapping team's “Low” thresholds could be included as minimum criteria in our requirements. This should address the concern over having a “negligible” ranking without requiring us to have an explicit 'negligible' impact category.
3. Are the 'R' statements at the right level? In the current CIP-002, each asset category has its own 'R' statement but we think this is unnecessary.

In terms of next steps he noted the subgroup would:

- Convene the remainder of our team to gather input and wordsmith our requirements.
- Obtain and incorporate the work of the Reliability Functions team into our requirements.
- Work with the Mapping team to determine minimum requirements for our lists.

BES Mapping Subgroup leader John Lim noted they met twice since Vancouver and have reviewed and used/borrowed concepts from three key documents: a set of critical asset

guidelines; the NERC DHS proposal for tiering BES assets (3 tiers) depending on impact on reliability of BES; and a classification of events. The resulting first draft of Requirement #2 will address how responsible entities will apply set of criteria to map list from requirement to high/medium and low tiers. The Subgroup is still debating this but it appears that there is a fundamental problem with hard thresholds. While there is more work to be done, it appears that High impact is the most important to be clear on, then Moderate impact. And then all else remaining may be in Low.

On day two John Lim presented the Subgroup's report noting they have lively discussions in the last few days. Changed the format to a matrix for a number of assets in 3 sections: Control Centers and Back up Control Centers; Transmission; and Generation. There was a general aversion to thresholds. If we have to use thresholds, provide the way for entities to say if I meet the threshold with engineering analysis. The common thread is that this will require a lot of use of engineering analysis. John will take last 2 days of discussion; redraft the standard requirement format previously to reflect the discussion. He noted the following issues as outstanding: coordinating with the first 2 groups: functions and BES subsystems. Have a session with Phil Huff to ensure consistency with analysis in both groups.

Phil Huff presented a report on the Cyber Analysis Subgroup's work since Vancouver. He reviewed the 3 teams the Subgroup has formed: Cyber impact categorization; target of protection team; and external cyber systems. Phil reviewed the inputs and outputs of the Cyber System Categorization Process and described the objectives. Phil Huff presented the subgroup report on day 2. They are looking at functional impact. For example in terms of generation — what does it mean for cyber system to impact generation at a h/m/l. What does it mean to affect situational awareness? Short of detrimental, moderate, no impact.

Joe Doetzl presented the subgroups ideas on Target of Protection noting they are proposing to expand the scope of what needs to be protected, e.g. collateral system. The hope is that if we are able to apply the appropriate controls, it may take care of target of protection.

Frank Kim presented on requirements for external cyber systems and presented the issues for consideration. Most External Cyber Systems or Third Party Data Connection NERC CIP-related compliance areas are not thoroughly covered in the existing version of the Standards. Therefore further clarification is required. Amplifying External Third Party system, user, and agreement security considerations are further detailed in other industry security standards such as ISO 27002 and NIST 800-53 that could be leveraged for future iterations of the NERC CIP Standards that pertain to external third party system security. On External Cyber systems, if 2 registered entities with cyber connections then some arbitration agreement should be in place to define the assurance. Assurance is provided by NERC. Putting that over to security controls not in CIP 2 version 3.

Keith Stouffer presented the Definition and Selection of Controls Subgroup's work since Vancouver noting that he had hoped to have a set of controls for the SDT to review but hasn't had a chance to do that yet. On day two Keith Stouffer presented the review of ISA 99 Work.

They looked at controls in draft — voluntary standard. Some controls watered down and may not be useful. Looking at 800 53 controls as they may be more applicable to current environment. Proposing to keep same general CIP-003-009. Should 5 and 7 combined? Contained ½ or 2/3s of all requirements. Decided to propose keeping CIP-005 and make it electronic asset controls. The subgroup is fleshing out new CIP-005 to serve as a model for what the SDT will ultimately do with the rest of standards. Starting with 1 requirement from 800-53, R1 Account Management, they came up with low medium and high.

The chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP-002 which we can refine in November and December. She thanked the members for their hard work together and in the subgroups and encouraged them to continue working to make headway on each of their charges. She noted she would forward to the chair of the Standards Committee a statement on behalf of the SDT relating to TFE and the urgent action process. The SDT adjourned at 2:45 p.m. on August 21.

I. INTRODUCTIONS, AGENDA, AND SDT WORK PLAN REVIEW

The Chair, Jeri Domingo-Brewer and Vice Chair, Kevin Perry welcomed the members and Joe Bucciero conducted a roll call of members and participants in the room and on the conference call (*See appendix #2*). The Chair reviewed the meeting objectives and Bob Jones, facilitator, reviewed the proposed meeting agenda (*See appendix #1*). The SDT adopted the July 13–14 meeting summary without comment or objection on Friday morning.

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

Vice Chair Kevin Perry announced, effective at end of October meeting, he will be stepping away from the SDT due to his responsibilities with his new job. He noted he will miss working with the team which has been a superb group to work with. Following the meeting, Mr. Perry asked that the following additional comments be shared with the SDT and placed in the meeting summary: “I believe there are four principles to bear in mind as we develop the new standards requirements: Remove variability; Remove arbitrary decision making; Criteria (requirements/controls) must be clearly understandable; and Criteria performance must be auditable - the entity must be able to demonstrate compliance. As we go through this process, step back and ask yourself two questions: 1) as an entity, how would I comply with the requirement and demonstrate my compliance? 2) As an auditor, how would I confirm compliance?”

Mr. Langton reviewed the CIP-002 work plan between August and December 2009 which the SDT adopted at its meeting in Vancouver, setting up subgroups and some ground rules for their work and coordination with each other. The monthly agenda planning meetings with the chair and vice chair have been expanded to include a leadership coordination meeting with the leads from each of the five subgroups. He noted the five subgroups have about four months to finish work of developing the CIP-002 draft to be released for industry comment in December 2009. He noted by the conclusion of the October 2009 SDT meeting, the goal is to have a single draft CIP-002 that can be debated and refined in November and adopted in December.

Jeri Domingo-Brewer briefed the SDT on the chair and vice chair’s presentation to the Standards Committee on a conference call earlier in August. They noted the SDT’s appreciation for the ongoing significant support for their work. When the Committee members indicated concerns with the length of the schedule, the chair indicated the SDT’s plan is to have the bulk of their work done by the end of 2010. The chair and vice chair agreed with the Standards Committee that the SDT needs to make significant and visible progress or its effort will be overtaken by events and efforts outside the industry. Finally the Committee asked the SDT leadership to provide them with a “heads up” if there are any issues that might affect the SDT’s ability to get the job done in a timely fashion.

II. UPDATES

A. Technical Feasibility Exception (TFE) NERC Rules of Procedure Posting

1. Introduction

Kevin Perry made the presentation and Scott Mix, NERC offered additional information. Mr. Perry noted the work of the NERC “Tiger Team” led by Mike Assante, NERC Chief Security Officer, with regional entity representatives to address a number of issues that have been raised in the industry comments received to date. Scott noted that the plan is to submit to NERC Board of Trustees for review and adoption at the October meeting following its consultation with the regional entity representatives. NERC BOT hopes to adopt a final TFE process sometime next year to submit to FERC.

2. Review of Initial Proposals for Addressing TFEs.

On the first day the SDT discussed the current situation with the TFE process and whether the SDT should support efforts to find a standards solution approach to the challenge presented by TFE interim process in advance of the adoption of CIP Standards Version 3. Mr. Perry noted that NERC’s current view is that explicit or implicit “enabling language” references in the CIP standards will be required for an entity to request and receive a TFE. NERC came out July 1 with interim guidance. The ROP put out for comment has received significant comments and concerns. There is currently no program and process in place to support the guidance. Regional Entities are asking the industry entities to hold off submitting their TFEs until this is sorted out. Regional Entities have proposed to take over the processing of TFEs and final touches on a joint NERC Region proposal (“Plan C”) are being made. It will call for TFE requests submitted to regions in 2 parts. Part A: identification type of equipment and issue and why the TFE is needed. Part B. will require a “deep dive” into how the mitigation plan will appropriately protect grid in absence of strict compliance. The current TFE proposal today would limit the applicable requirements to 14 requirements and sub requirements in CIP-005, CIP-006, and CIP-007.

If you have a compliance issue other than those requirements where a TFE is available, there is a 90-day schedule. Regions have 60-days to triage the TFE requests and determine whether to conditionally accept them: 1. Saying yes and give an exception or 2. Telling the entity to try again, and why they are being rejected. The entity will have one opportunity to revise and resubmit the TFE request in 30-60 days. If provisionally accepted they will be granted safe harbor from compliance action. If you fail to do anything promised you may lose safe harbor, e.g. not maintaining the mitigation plan — and it goes back to initial request date for compliance. Regional Entities are not currently staffed to do this. The TFE Process is supposed to hit the streets next week for an abbreviated comment period. Mr. Mix noted that the initial 60 days is extendable subject to approval by NERC. Also it was clarified that there could be multiple rounds if done within 30 days.

Kevin Perry presented a proposal that the SDT consider a relatively focused and narrow effort to propose standards changes undertaken by a small team of SDT members to build upon the

“Technical Feasibility Exceptions Matrix of Applicable Requirements” (see Appendix # 6) that he and other in the industry have been developing. It would propose a broader interim TFE process that will allow for a safe harbor for technical feasibility exceptions granted in the interim. An alternative proposal, presented by Gerry Freese, would propose creating a broader effort that would address the TFE and other interpretation issues raised by CIP Version 1 and Version 2.

The SDT then identified the following pros and cons related to the TFE proposals:

Pros	Cons
It addresses an urgent issue confronting the industry that may undermine the effectiveness of the SDT in producing a CIP Version 3 the industry will adopt.	It will divert and dilute SDT time and resources and time to getting the CIP 002-009 version 3 done ASAP
The SDT is best positioned currently to get this job done	The SDT may have to adjust and lengthen its Version 3 CIP schedule to respond to industry comments and engage in the ballot process.
Shows FERC and congress the industry is doing something in the interim before Version 3 adopted and approved by FERC.	The Standards Committee has asked the SDT to move as expeditiously as possible to complete its charge
	The SDT will address and seek to minimize the need for invoking TFEs in the CIP Version 3 conceptual approach and should focus on that.
	May result in further confusion about the relationships among the NERC ROP, Version 3 SDT standards development process, the Version 2 guidelines and the TFE Interim Guidance and the permanent process.
	May appear to Congress, FERC and others that SDT resources are being redirected to deal with TFEs
	Expanding the TFE process to address other issues will be difficult to fend off industry members who will want to see the rational for not addressing others.

Member Discussion Comments on Proposals Day One

- There is confusion on the status and the development of the TFEs. The initial draft ROP Scott Mix worked with the SDT on. Lawyers got involved. Regions didn’t like the approach to the process. Concerned about entities and audits. Struggling how to deal with practical things. What are entities allowed to do with the TFEs?

- NERC needs to make this simpler — for asset owners and members so they can get their jobs done and spend more time thinking about good security in grid. Good security on grid is possible.
- Should there be any limitations for when you ask for a TFE? Why not provide that TFEs can be requested for all requirements. Let each be reviewed and stand on the merits. If it will mean more work for NERC and the regions, so be it.
- Is the position that the TFE exception, unless explicitly authorized, is not allowed supported by FERC staff?
- Concerned about Congress' perception of the industry diverting resources/efforts away from the reform of the 002-009 from Order 706.
- Mr. Perry sent matrix around seeking input from TFE tiger team and the CIP auditors in other regions. The current draft reflects consensus of opinion across the regions as to areas one should be able to take a TFE. NERC however has not accepted it. FERC did not state in Order 706 that TFEs only could be taken where explicitly set forth in the standards. In fact in May, FERC staff suggested they envisioned broadening the ability of TFEs. However FERC legal and NERC legal have developed a different opinion leaving the industry stuck between a rock and hard place.
- Industry folks are increasingly asking SDT members to explain the rules. Hard to describe where the process is: first had a SDT proposal, then a NERC proposal, then a regional proposal. Don't know what the rules are. Bottom line- people in industry will do everything they can, but are concerned about getting caught in the confused mess. Risk is great with this much confusion.
- Other things in the original proposal. Issues of criteria on safety for e.g. If you have a safety issue it is valid? But only applies to certain requirements. Go ahead because don't care about the safety issue?
- Question from 1 region — making security policy reasonably available to everyone. E.g. Janitor — give him the entire policy. Translation. Supervisors do this. Laudable to put clarity into the standards. Keep in mind. Take hard look from entity's perspectives how to comply — look at auditors' perspective — how to verify compliance without an onerous.
- Distressed if CCWG focusing on this? Have regional compliance entities lost focus?

The Chair and facilitators suggested that this proposal be tabled to review on day 2 when the facilitators could summarize the pros/cons and work with the chair to develop a potential way forward for consideration by the SDT.

3. TFE Urgent Action Proposal

On Day 2 the chair mentioned that she and the vice chair reflected on the TFE day 1 discussion over dinner last night and offered an alternative proposal for the SDT consideration. Mr. Perry noted he was withdrawing his proposal from day 1 and proposed an “urgent action” path for TFE changes to the CIP standards. He included the following points:

- The SDT should express support for the use of the NERC Urgent Action process to address the current TFE dilemma as was done with the 1200 standard.

- In the Urgent Action process: someone drafts both a SAR and a modified standard that SAR covers and submits to the Standards Committee for their consideration. It differs from regular procedure in several respects. If the Standards Committee concurs, they will appoint a team and post the urgent action standard language for pre-ballot review followed by ballot and pre ballot.
- The Team will respond to comments from first ballot. If adopted by industry it goes to NERC BOT and to FERC.
- The urgent action standard will remain applicable for a set period of time but can be extended annually. A permanent standard must be placed in development to replace the urgent action standard.
- A major advantage to this approach is it doesn't distract the SDT from pursuing its charge.
- The Standards Committee might form another team, perhaps it is handed off to Larry Bugh chair of the original Version 1 SDT who has now completed the work with VSLs.
- It addresses the timeliness issue since the team is asked to do this it would respond only to comments following the first ballot. It does bypass collaborative nature of normal standards process.
- Mr. Perry briefly summarize scope for urgent action contained in the matrix (*see Appendix 6*)

Member Discussion of the Urgent Action Proposal and Matrix

- Did SDT have in mind covering the non-technical reasons in FERC order, safety etc. or strictly the technical?
- Mr. Perry spoke with NERC and urged them to figure this out. Non-technical exceptions treatment is inconsistent. NERC's paper currently has it both ways.
- How much time would it save if we took matrix and go and file without going through urgent action. Doesn't think it will take much time to draft? The mandate for posting for comment, accept, respond to comments, go out for pre-ballot review, respond to 1st ballot comments. We would have to follow all normal action process and it would take many more months and effort if there are significant comments.
- Why won't NERC accept the matrix? Standards Committee may say this is rewriting the standards outside the standards process.
- With the December compliance deadlines for generation folks, how long will this take?
- It will depend. Standards Committee must appoint team to handle the balloting process and they must respond to balloting comments. Post for pre ballot review. Best of all possible worlds. 10 day initial ballot period. 10 business days- only comment response. Not proposing difficult to understand issues. Industry won't be concerned where we are not making. 30 day posting, 30 day balloting. BOT review. Expedited board action. 30 days. Filing submitted to FERC.
- Upon board approval- standards are mandatory but not sanctionable.
- The generation folks will join the pool of entities that already are out there that in absence of TFE, will not be in compliance. That's why the urgency.

- Original intent of the Urgent Action process was to address situations that had an immediate impact to bulk power. Not to provide relief to standards however poorly written. Technical, operations and safety called out in the FERC Order 706. Is this the right use of the urgent action process. I don't believe it is.
- Scott Mix quoted the Urgent Action opening paragraph indicating intent for the SDT: "Under certain conditions, the Standards Committee may designate a proposed standard or revision to a standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed standard or revision can materially impact the reliability or security of the bulk power systems or be inconsistent with statutory or regulatory requirements for reliability standards, such as by causing adverse impacts on markets or undue discrimination. The Standards Committee must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or implement a standard." Pg 26 of http://www.nerc.com/fileUploads/File/Standards/RSDP_V6_1_12Mar07.pdf
- We shouldn't worry about the industry approval for this. It should be presented as a valid reliability issue. What will entity do with equipment they might have to replace because of TFE can't get. Submit SARs with standards.
- The expectation will be that when an entity is found out of compliance they will go through investigation, confirmation, plan, self-report and take steps to becoming compliant. Will have some form of reliability impacts. Standards Committee understands the issue.
- What's the alternative? The industry needs to do this. Even if helping a smaller group than all. I would vote to head in this direction. The TFE process is important to fix.
- This will help all entities. RC, Vas and TOPs are in need now. But others will be affected going forward. TFE needed? Spoke with head of his compliance. ERCOT would probably be very supportive and other ISOs would be support.
- The SDT needs to be careful and aware of the "optics" that may be seen as way of avoiding the process.
- The SDT could decline the opportunity to take this on because interferes with our mission and charge but support any efforts to take an Urgent Action approach.
- We are looking at the very best April 1 of 2010 of effective date of Version 2. Assumes FERC issues an order by end of September. Urgent action would not become effective until April 1 2010.
- This could mean that the requirements are enforceable but not sanctionable? Regions would take TFE requests for new requirements.

The facilitators noted this was an important issue and there seemed to be support for the SDT to help in some way to facilitate a solution. They presented for SDT consideration the following draft SDT Resolution:

The SDT supports the streamlined treatment of the interim TFE standards issues through the NERC Urgent Action Process utilizing the "Technical Feasibility Exceptions Matrix of

Applicable Requirements” (see Appendix # 6) as a basis for developing a discrete set of proposed modifications to CIP Version 2 standards.

Following some discussion of the resolution language, the Chair suggested that instead she draft a statement to the Chair of the Standards Committee which should note that the SDT has identified an urgent challenge for the industry and that the Standards Committee should consider how to address the gaps that have been identified in terms of Version 2 of CIP Standards and the proposed TFE procedure. The statement would note the SDT looked at trying to help with a solution given the skills, abilities and experience on the Team, but the time needed would take away from the SDT’s main charge and ability to complete the current work plan in a timely fashion. It could be sent to Scott Henry Chair of Security Committee, copying Dave Taylor and Gerry Adamski at NERC. This would be consistent with the Committee’s request that the SDT give them a heads up on challenges. The Vice Chair offered separately to bring SDT concerns to the NERC TFE group that was meeting by conference call later in the day.

The team agreed by common consent that the chair should prepare and send a statement consistent with the spirit of the SDT’s review and discussion.

B. VSLs and VRFs

Scott Mix reported on Dave Taylor’s behalf that Version 1 is complete with a 92 percent quorum and 84 percent approval rate. This has been submitted to FERC on July 30. It will be adopted by FERC rule or by NOPR. Version 2 VSLs and VRFs is in the 30-day pre ballot review period. The expectation is for the second ballot to conclude in early October.

NERC anticipates that FERC will take action on the CIP version 2 standards in September/October 2009 as an Order or a NOPR.

C. Update on other Related Cyber Security Initiatives

The SDT Webinar is scheduled for next week. Phil Huff described the presentation 20–30 minutes leaving 1 hour for questions and discussion. It will introduce the industry to the concept paper. As of today over 240 have registered. Phil agreed to send slides to SDT members. There will be a “dress rehearsal” before the webinar.

SDT Member Comments

- Confusion of concept paper with the Critical asset identification guidelines which a working group has out for wide industry comments.
- Part of CIPC package for its September meeting. Will include a redline and comments and response. Working group working on companion critical cyber asset identification.
- Confusion in the industry is running rampant. Mixed up between the two- follow concept paper for audit. Transmittal letters.
- Went back through the document — couldn’t find where this is roadmap for CIP-002 for version 3. May need a disclaimer on there.

III. CIP 002 SUBGROUP REPORTS TO THE SDT

A. Overall

Scott Mix noted that the SDT should begin focusing on both the content and format of a NERC standard. He mentioned he had discussed with Dave Taylor to possibility of a short set of clear requirements backed up by more detailed appendices or attachments. He noted that this would be a departure from how NERC normally does standards and that the sooner the SDT can get some samples to NERC to review format and structure the better.

Member Comments

- Do other standards have attachments associated with them? Scott reported that is precedent in that there are 8-10 standards that have attachments, e.g. EOP 2 (EEA Attachment) and IRO 6 (TLR procedures as an attachment).
- The functions group may have a proposed format to present to the SDT for their section by the end of the meeting.
- It will also be important to be able to show the flow and linkages from one requirement and any supporting appendix to the next

The Chair reviewed with the SDT the subgroups and their members and observers.

Subgroup Name	Members and Observers
Reliability Functions	John Varnell (1), Jim Brenton (1), Dave Norton, Rich Kinan, Doug Johnson, James Bassett
List of BES Subsystems and/or BES Cyber Systems	Jackie Collett, Scott Rosenberger, Jay Cribb, and Gerry Freese.
BES Mapping	John Lim (1), Jeri D. Brewer (1), Dave Revill (2) Sharon Edwards and Kevin Sherlin
Cyber Analysis	Chris Peters, Phil Huff, Rob Antonishen, Frank Kim and Joe Doetzl. Sam Merrell and Mike Toecker
Definition and Selection of Controls	Kevin Perry, Bill Winters, Jon Stanford, Keith Stouffer. Peter Schneider

B. CIP 002 Subgroup Reports and Discussion

1. Reliability Functions Subgroup Report

a. 8-20 Progress Report

John Varnell reviewed a draft list of assets the Subgroup was developing. He noted they haven't added any more functions but did combine some functions and expand on what was meant by each. He noted they hope to have a complete list by the end of the meeting.

Member comments

- Not sure we are all is clear on what each subgroup is to do and produce. Our group has come up with wording for a strawman for requirements would be worded and how functions would be used in the wording of the requirements.
- This subgroup will come up with list of functions. E.g. Requirement 1 in CIP 002 is to come up with list of BES subsystems. Need to list the functions and use list to come up with inventory of relevant subsystems. This might result in a list of minimum types of sub systems that must be used.
- Requirement 2 is the categorization itself and then onward.
- This subgroup will need to work with and help the BES Subsystems/BES Cyber systems Subgroup to come up with list of subsystems.

b. 8-21 Progress Report

John Varnell presented the following proposed functions critical to the reliable operation of the BES:

Defining Functions critical to reliable operation of the BES

The following functions must be evaluated by each Register Entity (RE) for all functions that the RE is responsible for as identified by the NERC Functional Model. The RE must identify ALL equipment required to perform the function, not just the RE owned equipment!

1. Dynamic response
2. Balancing Load and Generation
3. Controlling Frequency (real power)
4. Controlling Voltage (reactive power)
5. Managing Constraints
6. Control & Operation
7. Restoration of BES
8. Situational awareness
9. Inter-Entity coordination and communication

1. Dynamic Response

1.1. Spinning reserve (contingency reserves)

- 1.2. Governor response
- 1.3. Protection System (transmission & generation)
- 1.4. Special Protection System
- 1.5. Under frequency relay protection
- 1.6. Under voltage relay protection
- 1.7. Power System Stabilizers
- 2. Balancing Load and Generation**
 - 2.1. Load management
 - 2.2. Demand Response
 - 2.3. Load shedding
 - 2.4. Unit commitment
 - 2.5. Non-spinning reserve(contingency reserve)
 - 2.6. Calculation of ACE
- 3. Controlling Frequency (real power)**
 - 3.1. Regulation (regulating reserves)
 - 3.2. Generation Control (such as AGC)
- 4. Controlling Voltage (reactive power)**
 - 4.1. AVR (Automatic Voltage Regulation)
 - 4.2. Capacitive and Inductive resources
 - 4.3. SVC (Static VAR Compensators)
 - 4.4. Synchronous Condensers
- 5. Managing Constraints**
 - 5.1. Interchange schedules
 - 5.2. Generation re-dispatch and unit commit
 - 5.3. Identify and monitor SOL's and IROL's
 - 5.4. Identify and monitor Flowgates
- 6. Control & Operation**
 - 6.1. All methods of operating breakers and switches (such as SCADA)
- 7. Restoration of BES**
 - 7.1. Blackstart restoration including planned cranking path (nuke?)
- 8. Situational Awareness**
 - 8.1. Monitoring and alerting (such as EMS alarms)
 - 8.2. Change management
 - 8.3. Current Day & Next Day planning
 - 8.4. Contingency Analysis
 - 8.5. Frequency monitoring
- 9. Inter-Entity coordination and communication**
 - 9.1. Scheduled interchange
 - 9.2. Facility status
 - 9.3. Operational directives

He noted that there are no preconceived notions of regions as these don't exactly match current reliability standard requirements. The subgroup also changed some names so as not to confuse with other terms.

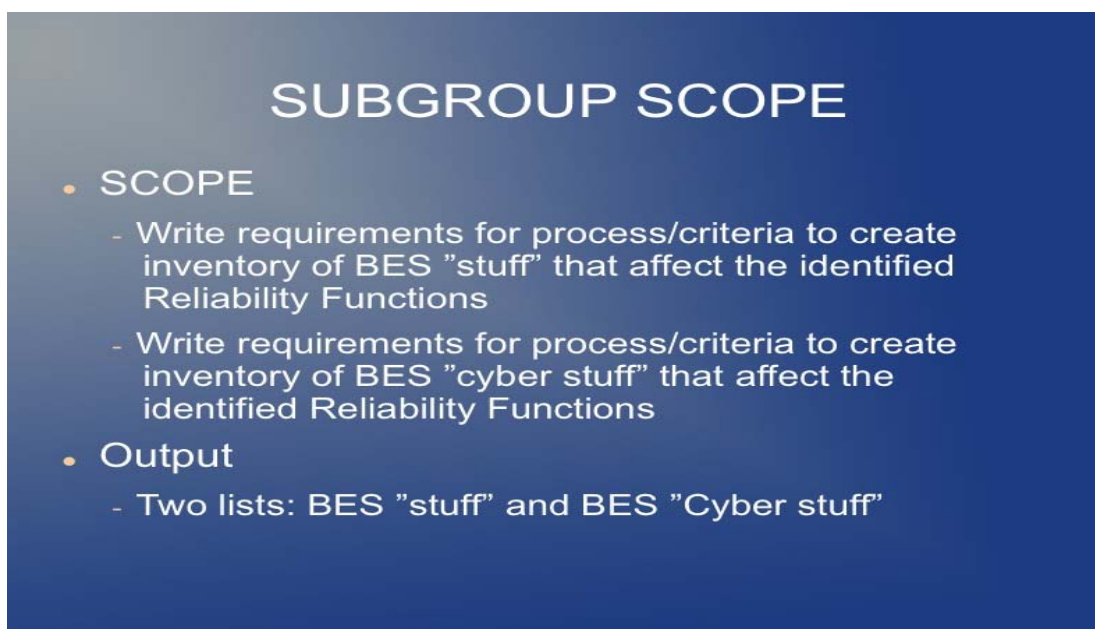
Member Comments

- It is a good idea to put numbers on everything to be able to follow this as we add detail, if necessary. Use numbers to refer to specific functions. Attachments to standards- will be consistent across all entities.
- Why the calculation of ace and not ACE and load balancing? 4. Synchronous condensers here? Yes.
- ACE is specifically laid out in the standards. It is a piece of balancing load and generation.
- Looking at functions based on impact on BES. Thought it might be clearest way to identify the functions.
- The subgroup will develop the real thing and get the requirements. These are the categories the subgroup wanted to get out to other subgroups and their leaders so they can start out their pieces with some idea of the functions.
- Jason Mason offered to run by the Assist Team- OC meeting in September pass by them. The subgroup agreed this would be helpful.

2. List of BES Subsystems/BES Cyber systems Subgroup Report

a. 8-20 Progress Report

Jay Cribbs presented an overview of the work done since the Vancouver meeting. Jackie Collett was on vacation but the group met once in the interim. He described the subgroup scope and expected output.



SUBGROUP SCOPE

- **SCOPE**
 - Write requirements for process/criteria to create inventory of BES "stuff" that affect the identified Reliability Functions
 - Write requirements for process/criteria to create inventory of BES "cyber stuff" that affect the identified Reliability Functions
- **Output**
 - Two lists: BES "stuff" and BES "Cyber stuff"

He noted the subgroup has identified a list of issues and questions (“in this phase the subgroup is coming up with all questions and no answers”) that will guide their efforts to develop draft requirements:

- We're step 2. What is step 1's output? Meet with Reliability Functions team to see what their output consists of.
- How do we handle system that cross functional model entities or is owned/controlled by different entities? Whose list does it go on? What if different entities assess things differently?
- What is the definition of “system”? What is the proper granularity of system identification? Must provide clarity not confusion Focus on “stuff” for now then we'll determine the right terminology that considers the NERC Glossary.
- Will there be minimum criteria to be on the lists? This is not an asset management system how do we insure complete list without requiring everything?
- What is the methodology for identifying BES and cyber assets? How do we write a methodology in a requirement?
- Are assets in “connections” to be included in the lists, or do these come in later in the TOP?
- How to handle the dynamic nature of the grid?

SDT Member Comments

- The interface requirements underscore the coordination effort that is critical re output and input.
- This subgroup is the first requirement.
- What is definition of “system”? What level of granularity is needed to define /identify system. Provide clarity not confusion.
- Minimum criteria- to be on list? This isn't an asset management system. Don't want to require everything but where is the line?
- Will there be things like generation at some level or higher?
- What will be the methodology for identifying BES? How to write a methodology in a requirement will be challenging.
- Assets in connection to be included? Target of Protection team will handle.
- One of the things the functions group has discussed. Will have some problems with not having said anything about the overview of the area/region and not being the regional coordinator. This will be challenging all the way through.
- The OC/Planning Committee nominees are now organized and up to speed. They have been given them the list of contacts of the subgroup chairs. The first 3 subgroups groups will be most applicable.
- Can't meet external reviews in the FERC order.
- We hope to be looking at established or establishing thresholds for classification in order to eliminate need for external reviews. Conflicts with RCs. Wrong guesses= liability. This may no longer applicable given new approach. What they ordered was tweaking the existing standards not a rewrite.

- This doesn't mean the RCs are completely out of picture. Criteria may be based on criteria set by RCs. E.g. Contingency reserves set by RCs? That is a BA function or an RSU function? RC can provide insight and information which is different from oversight and review.
- You don't need to know what kind of control system, just know what things required to make the system work reliability.

b. 8-21 Progress Report

Jay Cribb presented the Subgroups report on day two offering the following points:

- We will not outline the process for "how" to create the lists. The white paper gives flexibility in the creation of the lists and allows entities to take a primarily cyber systems oriented view if they wish.
- Assets and systems that are below the mapping team's "Low" thresholds could be included as minimum criteria in our requirements. This should address the concern over having a "negligible" ranking without requiring us to have an explicit 'negligible' impact category.
- Are the 'R' statements at the right level? In the current CIP-002, each asset category has its own 'R' statement but we think this is unnecessary.

In terms of next steps he noted the subgroup would:

- 1) Convene the remainder of our team to gather input and wordsmith our requirements.
- 2) Obtain and incorporate the work of the Reliability Functions team into our requirements.
- 3) Work with the Mapping team to determine minimum requirements for our lists.

3. BES Mapping Subgroup Report, Q & A

a. 8-20 Progress Report

John Lim, the Subgroup leader noted they met twice since Vancouver on August 5 and on August 19. They have reviewed and used/borrowed concepts from three key documents: a set of critical asset guidelines; the NERC DHS proposal for tiering BES assets (3 tiers) depending on impact on reliability of BES; and a classification of events. The resulting first draft of Requirement #2 will address how responsible entities will apply set of criteria to map list from requirement to high/medium and low tiers. The Subgroup has sorted and put the requirements in 3 buckets as an initial exercise. The Subgroup is Still debating this but it appears that there is a fundamental problem with hard thresholds. E.g. 2000 mw, doesn't make sense unless you have an analysis backing that up in terms of impact on reliability. Key need is an analysis to support or not for a bright line threshold. In general, they are trying to get away from hard thresholds. Will be probably qualifying requirements based on this analysis. While there is more work to be done, it appears that High impact is the most important to be clear on, then Moderate impact. And then all else remaining may be in Low.

SDT Member Q & A/ Comments

- How were the levels arrived at? SGWG critical guidelines? Took from 3 documents.
- What is status of the NERC/DHS document process?
- Other criteria were taken from the guideline at the time it was published. Will recheck with final document submitted.
- Members comments on the work. Rod joined from the SIS with good input.
- Subgroup gather together these documents as some of ways to look at criticality. Only begun to vet. Member companies have vetted. Next steps on vetting.
- While there were initially 19 measures for assessing criticality, the subgroup hopes to condense them down to a handful.
- Vetting with SDT- seems to be a resistance to a numerical thresholds. All but 5 members expressed concerns/problems with numerical thresholds.
- 1st requirement. 2000 mw? Is there a way to determine that is universal, and standardize that so that it is not up to a company to figure out?
- Dilemma is you need clear criteria to allow entities to make the correct determination of level (e.g. high). Haven't yet got to the point of how to handle this. This is a threshold, unless you can demonstrate through engineering analysis etc. that it is not. Is it "high unless demonstrate it is not high?"
- Congress won't believe that 2000 mw is not critical. If this were the threshold it wouldn't fly.
- The issue shouldn't be is 2000 the right number, but are big generators critical? Then focus on what "big" is in different interconnections, regions. Sound engineering based on what "big" is and document it in an attachment. It will have to be persuasive. Note that it may make sense in eastern connection and irrelevant everywhere else.
- Big transmission stations- how much is lots of stuff, and what is stuff? John Lim's group will have this job.
- Sharon questioned whether thresholds good. Want to know what the impact is on the BES. Don't care for e.g. lose generation in sharing event exceeding contingency reserve level. Focus on how does it impact the BES. Not thrilled with the tiers. Need to keep in mind the on potential for cascading. There is fear about what "misuse" means. E.g. Aurora turned off a bunch of protections to use this.
- It is important we cover not just the loss of but also misuse of an asset. Operators don't have a long history this.
- How big is big is going to be different in different areas. RCs are going to be the ones understanding this. Not just for oversight but for definition before oversight. Need to discuss this sooner than later.
- To extent you can define common mode contingencies, RCs can provide that guidance.
- Any threshold is wrong. Being big is not the right question. Transmission planner for 11 years. Size of substation or generator. Has to be room evaluation and rational decision that would avoid inconsistent answers in different regions.

- Differences between different regions are presently handled by event analysis. Do other standards have differentiation among the regions?
- Keep in mind “small guys” in the low impact category. Any thing will be weighed against NIST menu of controls.
- Do we need to look at a “non applicable” or negligible category?
- All cyber assets need some level of protection. Thresholds may not be the way to go. Address the different thresholds among interconnections. Those are going to be dynamic and change on a temporal basis and thresholds will be affected by that.
- Mike Assante’s- protect control systems in general, large, medium and small.
- Even a small asset with connection needs to be protected. Be careful about what we say should and should not be protected.
- Perception out there may be driving this- if you have a big piece it has to be critical or high impact. If freedom given to reach those determinations then we have the materials to address them.
- VRF team- tendency to call “high” because it is part of standard. This is similar. Don’t rush to categorize as high impact as there will be implications down the line.
- Appreciate the SDT feedback- importance of being able to assess the impact to the BES as they are the driving focus of what we are trying to do. If anyone has any across the board strategies we are all ears. What is the best approach to do this? John Lim’s approach was valid as a starting point. When you look at these individually they are very flawed.
- Recognize system dynamics causes daily changes. Got to remove variability aspect from any criteria we have. Shouldn’t change way we view impact on BES.
- Remove arbitrary decision process that we have today, understandable, repeatable and makes sense. Get away from entity gets to make that choice.
- What ever performance criteria developed- can demonstrate compliance.
- Hard limit on generator output as a threshold related to BES reliability? Balancing generation and load when they get out of whack, they can become a real problem overtime.
- How you can address control systems of neighbors. RC can’t really do this. This is a hole in our concept.
- Inadvertent interchange- can be a good thing, not necessarily a bad thing.
- BES Asset and associated cyber stuff. High, medium low. Concerned about time needed to come up with thresholds vs. set of controls applied to everything.
- Focus of NERC and FERC has been on documentation. We potentially have a system with sanctions for something that is not important to reliability.
- The schedule proposed to implement a security control may be different/ (shorter or longer) if it is a high, medium or low impact. E.g. 2 years for high, medium 5, lows 10. 10 year plan. Prioritize work. Keith Stouffer and the Controls subgroup work may help.
- Assign VSF/VSL differently to high medium low?
- References entities criteria be arbitrary? Variable maybe. Not as arbitrary as a threshold standards. N-1 methodology- look at extreme events not N-1- TPL standard

studies include more than N-1. Include contingency events in terms of terrorist actions. Concerned about global national thresholds.

- Differences in controls in the baselines. Some are same, some different. Access control suite of family. Low has 11 requirements; moderate 34 requirement/enhancements; high 39 requirements.
- Awareness and training- same across the board.

b. 8-21 Progress Report

John Lim presented the Subgroups report noting they have lively discussions in the last few days. Changed the format to a matrix for a number of assets in 3 sections: Control Centers and Back up Control Centers; Transmission; and Generation. The subgroup discussed what are control centers, discussed thresholds whether they should be yes/no or performance based. There was a general aversion to thresholds. If we have to use thresholds, provide the way for entities to say if I meet the threshold with engineering analysis. The common thread is that this will require a lot of use of engineering analysis. What is it? Will be a challenge to formulate this to put in a standards requirement that is auditable. John will take last 2 days of discussion; redraft the standard requirement format previously to reflect the discussion. He noted the following issues as outstanding: coordinating with the first 2 groups: functions and BES subsystems. Have a session with PH- to ensure consistency with analysis in both groups. Call scheduled in early September- functions group invited to join.

SDT Members Q & A

- High. Medium and low for each category. Specific to another layer- table with 50 rows of h/m/l impact?
- Purpose of functions will be different. Higher level of granularity. Lower level functions useful in providing guidance to entities to identify who is doing what. Keep functions in mind when looking at criteria.
- If this will be auditable, you have a reliability function, go to table to find h/m/l and that is what you would share with the auditor.
- Single subsystem performing a high and lower function, will be placed in the higher.
- Need to be clear so there is no question as to how someone arrived at the rankings.

4. Cyber Analysis Subgroup Report, Q & A

a. 8-20 Progress Report

Phil Huff presented a report on the Subgroup's work since Vancouver. He reviewed the 3 teams the Subgroup has formed: Cyber impact categorization; target of protection team; and external cyber systems. He outlined some issues and assumptions including:

- Cyber analysis- impact assessment on the BES cyber system reliability function
- What impact do reliability functions have on the BES?

- Impact levels: perfect process with impact level the weak point in terms of verifiability.
- Impact levels for each reliability function. High impact to situational awareness, generation control.
- Most BES cyber system will likely have high impact on the function.
- Impact of information disclosure (CEII).

Phil reviewed the inputs and outputs of the Cyber System Categorization Process objectives as:

- To ensure the Responsible Entity categorizes all of its BES Cyber Systems according to the impact a violation in the Cyber System security requirements would have on the BES.
 - To correlate BES reliability functions directly to the BES Cyber System.
 - To correlate the objectives of protecting the confidentiality, integrity, and availability of the Cyber System directly to its BES impact categorization.
- The cyber impact categorization takes the high water mark of impact on each of the supported functions.
- State explicit criteria for the Cyber Impact Assessment (including the misuse of Cyber Systems) [*from the SDT Points of Consensus*].
- Include a methodology to merge the BES and Cyber Impact assessments [*from the SDT Points of Consensus*].

He noted the following issues the subgroup has identified for consideration:

- Impact levels or Cyber categorization are difficult to audit. The alternative to having generic impact descriptions would be to have specific descriptions for each reliability function.
- Assumption: Almost all BES Cyber Systems are *High* impact to the function they provide. If this is the case, then the Cyber Impact Assessment is trivial. This is equivalent to the BES Subsystem impact mapping determining the final categorization.
- In the paper, the cyber impact categorization ties to the final categorization through a matrix. The purpose of having a matrix is to provide some control in how an entity categorizes Cyber Systems. So the cyber impact categorization limits the view of impact only to the reliability functions it supports without considering the importance of those reliability functions to the BES. However, we define a BES Cyber System as one which directly supports reliability functions of the BES. One could argue that, by definition, all BES Cyber Systems have a high impact on the reliability functions they support.

- Instead of a matrix, we might consider using the BES Subsystem mapping as an upper bound which results in the following:

Asset Impact -->	High	Medium	Low
Cyber Impact:			
High	H	M	L
Medium	M	M	L
Low	L	L	L

- Cyber impact would have an upper bound of the function(s) it supports. Using this methodology, it would not be necessary to include the matrix within the Standard.
- We assume the BES Subsystem mapping will have (high/medium/low) criteria. If this is the case, then the Cyber Impact Assessment would look to the criteria for the loss of confidentiality, integrity and availability.
 - The BES Subsystem mapping provides input by mapping the worst case.
 - When assessing the impact of a Cyber System, the organization would first map all of the BES Subsystems which the Cyber System can impact.
 - The organization would look at the loss of confidentiality to a BES Subsystem, as an example. It should not have greater impact to the BES than the BES Subsystem impact mapping. However, justifying a lower impact category would be on the basis of the functional mapping criteria.
- Need to work with *Reliability Functions* team to ensure information such as CEII fits into the proposed assessment model.

He then noted the following steps:

- Step 1 — BES subsystem mapping, e.g. SCADA system.
- Step 2 — Assess the potential functional impact. E.g. what impact does SCADA have for every reliability function (blackstart etc.) E.g. Situational awareness.
- Step 3 — Combine in categorization look up table. Have BES mapping for functions.
- Step 4 — Final categorization. High water mark approach.

SDT Member Q & A

- How are you handling the aggregation issue? Mapping to BES sub systems. When multiple, taking a high water mark? Yes.

Joe Doetzl presented the subgroups ideas on Target of Protection noting they are proposing to expand the scope of what needs to be protected, e.g. collateral system. The hope is that if we are able to apply the appropriate controls, it may take care of target of protection.

Frank Kim presented on requirements for external cyber systems noting the following objective:

- Identify and manage risk associated with External Cyber Systems or Third Party Data Connections operating within the Target of Protection

He then presented the following issues for consideration:

- Most External Cyber Systems or Third Party Data Connection NERC CIP-related compliance areas are not thoroughly covered in the existing version of the Standards. Therefore; further clarification is required. In addition, industry security practices and controls such as modifying existing entity contractual agreements and processes to meet applicable NERC CIP requirements should be addressed.
- Amplifying External Third Party system, user, and agreement security considerations are further detailed in other industry security standards such as ISO 27002 and NIST 800-53 that could be leveraged for future iterations of the NERC CIP Standards that pertain to external third party system security. These are not necessarily germane to this requirement but several examples include:
 - **Security Assessment and Authorization (CA-3) Cyber System Connections**
 - Control: The Responsible Entity:
 - Authorizes connections from the Cyber System to other Cyber Systems outside of the Target of Protection through the use of Interconnection Security Agreements;
 - Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and
 - Monitors the Cyber System connections on an ongoing basis verifying enforcement of security requirements.
 - **Personnel Security (PS-7) Third-Party Personnel Security:** policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.
 - The Responsible Entity:
 - Establishes personnel security requirements including security roles and responsibilities for third-party providers;
 - Documents personnel security requirements; and
 - Monitors provider compliance.
 - **Supplemental Guidance:** Third-party providers include, for example, service bureaus, contractors, and other organizations providing Cyber System development, information technology services, outsourced applications, and network and security management. The Responsible Entity explicitly includes personnel security requirements in acquisition-related documents.
 - **System and Services Acquisition (SA-9) External Cyber System Services**
 - Control: The Responsible Entity:
 - Requires that providers of external Cyber System services comply with Responsible Entity Cyber System security requirements and employ

- appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Defines and documents government oversight and user roles and responsibilities with regard to external Cyber Systems services; and
- Monitors security control compliance by external service providers.
- **System and Communications Protection (SC-7): Boundary Protection**
 - Control: The Cyber System:
 - Monitors and controls communications at the external boundary of the Cyber System and at key internal boundaries within the Cyber System; and Connects to external networks or Cyber Systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

SDT Comments Q & A

- 3rd party connections not covered in the standards. Will ultimately require
- Borrowed from ISO 27 002, NIST 853.
- 2 types of external cyber systems- those under realm subject to NERC. Others not under NERC regulations but have some impact.
- Mix of 3rd parties: vendors, consultants.
- How far to go in 3rd party cyber systems? Should we go for a more narrow focus?

b. 8-21 Progress Report

Phil Huff presented the subgroup report on day 2. They are looking at functional impact. For example in terms of generation what does it mean for cyber system to impact generation at a h/m/l. What does it mean to affect situational awareness? Short of detrimental, moderate, no impact.

SDT Member Q &A

- However we make these decisions, important to capture the thought process. This is what we used to determine high, medium or low.
- Is the impact specific to the function and not the cyber?
- Aren't we looking to the reach of each cyber asset with the reach determining high/med/low
- What is the relationship of cyber asset to functions or sub-functions? The functions themselves dictate what the impact is.
- EMS e.g. impact is high water marking. If it touches 40 of 50, it is high, don't need to look at the other 39. Make sure as soon as you hit the high, you are done. This has to be clear to auditors.
- Target of Protection- security controls- not a requirement that goes in CIP 2 for this. Working hard on definitions in terms of consistency and intent in terms of BES and cyber systems you want to protect.

- On External Cyber systems, if 2 registered entities with cyber connections then some arbitration agreement should be in place to define the assurance. Assurance is provided by NERC. Don't need more.
- Issues with external cyber systems. Putting that over to security controls not in CIP 2 version 3.

5. Definition and Selection of Controls Subgroup Report, Q & A

a. 8-20 Progress Report

Keith Stouffer presented the subgroup's work since Vancouver noting that he had hoped to have a set of controls for the SDT to review but hasn't had a chance to do that yet. He hopes to start working on that soon and bring to the next session. The Subgroup needs help from the SDT on which requirements have the highest priorities that controls are needed for? The Subgroup will need guidance on which to do first and on to last. They have looked at ISA 99- 4 baselines (security assurance levels, and DHS Catalogue of Control System Security just a catalogue NIST 800-53, ISA 99

SDT Member Q & A

- Shows the connection with the ISA and NIST work as well as
- Mike Assante's Congressional testimony training and awareness, incidence response addressed at an organizational level.
- Pull out of catalogue controls and look at general requirements.
- In the Federal system can take care of some of these at organizational level
- From Policy at high org level down to specific controls, vary by installation or by system.
- SDT need to get arms around the consistent use of terminology. Lets refer to these as a "Catalogue of security controls" vs. the familiar process controls.

b. 8-21 Progress Report

Keith Stouffer presented the review of ISA 99 Work. They looked at controls in draft-voluntary standard. Some controls watered down and may not be useful. Looking at 800 53 controls as they may be more applicable to current environment. Proposing to keep same general CIP 003-009. Should 5 and 7 combined? Contained 1/2 or 2/3s of all requirements. Decided to propose keeping CIP 5 and make it electronic asset controls. The Subgroup is fleshing out new CIP 5 to serve as a model for what the SDT will ultimately do with the rest of standards. Starting with 1 requirement from 800-53, R1 Account Management, they came up with low medium and high R1 Account management e.g.

SDT Member Comments

- a and b used in making your documents. Why struck? Seemed odd. Will sort out.
- Exclusion #2 don't agree. Default accounts need to be authorized. Aware they are there. Should remove as well. Requirement for reviewing, for approving.

- The Subgroup had the same discussion among themselves.
- Changing the name of account is not changing the account. System id. Can't be changed. Name vs. the function/role.
- On the low 11 controls apply? On this one requirement of one standard. If there are no minimum then every asset is at least a low. Everything- with a chip in it. Is there no "lower than low"?
- I.e. a negligible category? Other piece trying to match requirement to the characteristics of the device and says you don't have to. Malware on an old relay.
- Already have 2 standards- as developing controls- document that says this is why we are not applying this.
- Minimum- utilizing exclusions to manage the "negligible"? 800-53 more extensive, and more guidance. Will be developing a guidance to go along with standard.
- Look at version 1 experience, following 2nd draft, had to take out word "exclusion"
- We should talk in version 3- 200-300 controls? Think about some formal presentation different variations. Formulate a way for dealing with exceptions. Consider controls
- R 1.5.3 remove access to the role, therefore can't perform in the role. Timeline needed here. Cover the entire populations of individual transferred. When someone leaves, remove access and then grant access again.
- Would you consider applying different levels- for high it will be removed. For a low we may not need to do.
- 1 hour termination- how audited?
- Implement system- termination person- within 24 hours. Need to provide documentation. Multi-million access control by profiles. Lots of resources to do this.
- Deletion of temporary-R1.2 f. striken.
- 1.5 sections - 10k switzer relays. 24 hours to change passwords- no inheritance of higher level controls.
- Have to look at environment has to be recognized in drafting controls and requirements.
- Current sub standards don't address this. Users that have access but are not authorized, e.g. system administrators. Need to clearly address.
- Timeline on transferred users etc. can't tell entity that in 1 week to something. "Removing unneeded access" simplifies.
- Technical merits- discussion is good.
- Concerned about this requirement- looks different from everything we've done as part of a standard.
- Get format in front of dt, ga, Maureen, compliance, legal.
- As soon we figure out what it will look like. How will it work? Can it be an acceptable NERC reliability standard.
- Had discussion. Will do what they want and then hear from NERC on whether or not it is possible. Get it down for one requirement. See if it is acceptable.
- NERC no longer putting Rs on sub requirements.
- Applicability and exclusions?

- Need to get Maureen in with this team ASAP.
- If applicability was at beginning- that would flow better than at end.
- Embed applicability in requirement language. Figure out how to draft the structure of the requirements.
- If requirement has sub requirement. Roll up requirements. E.g. the Entity shall do the following
- Some requirements have more than 1 within the requirement itself.
- If roll up function why does it have a VRFs? Have to have a VSL with the main requirements.
- We need to get a hold of filing- and look at Version 2. Such as—bullets. Kept sub requirement.
- Information “Filing” attach to the minutes. Jason will send.
- Need to encourage Maureen to produce a style guide. Scott will follow up.
- This requirement, consolidates all or parts several of CIP 4 R4, CIP 5 2.4.1 2.1.3,
- Is this drafting team going to develop VSLs for version 3? Yes.
- Encouraged by approach- getting all related to a functional area in one place vs. the spaghetti approach.
- Shouldn't have to do all standards at one time.
- Any areas identified where need communication coordination?
- 1 area- make sure opportunity for someone analyzing a function needs to i.d. all hardware used to perform that function whether they own it or not. Assets that do not belong to them.
- John Lim talked about that in criteria. E.g. generation and transmission owner context. Requirement for generator to notify your transmission owner and operators of impact level of facility.

VI. NEXT STEPS AND CLOSING

The Chair reviewed with the SDT the schedule for the next couple of meetings reminding members that at the conclusion of the October meeting in Kansas City we hope to have a single text of CIP 002 which we can refine in November and December. She thanked the members for their hard work together and in the Subroups and encouraged them to continue working to make headway on each of their charges.

She noted that she would draft up the letter to the Standards Committee Chair based on the SDT's discussion of the TFE and Urgent Action approach.

Members completed an onsite meeting evaluation form (*See, Appendix #3*).

The SDT adjourned at 2:45 p.m. on August 21.

APPENDICES TABLE OF CONTENTS

Appendix 1: Meeting Agenda	32
Appendix 2: Meeting Attendees List.....	34
Appendix 3: Meeting Evaluation Summary.....	36
Appendix 4: NERC Antitrust Guidelines	38
Appendix 5: SDT Work plan Schedule	40
Appendix 6: TFE Matrix of Applicable Requirements	43

Appendix # 1— Meeting Agenda

Proposed Meeting Objectives and Outcomes

- Review the work plan going forward;
- Receive update on the MRC presentation and Leaders Coordination call;
- Receive updates on TFE, VSL/VRF and related cyber security efforts;
- Receive and discuss reports from CIP 002 Subgroups;
- Convene CIP 002 Subgroup meetings;
- Subgroup reports back to SDT; and
- Agree on work plan, next steps and assignments.

Thursday August 20, 2009

8:00 a.m. – 12:45 p.m.

- 1. Review of CIP 002 Work plan and Subgroup Process including pros – cons of a possible TFE Exception “Version 2.5” — Kevin Perry and Jerry Freese’ Version 2.5 Proposal**
- 2. Update on Technical Feasibility Exception (TFE) NERC Rules of Procedure and VSLs – VRFs**
- 3. Subgroup Reports to the SDT**
 - Reliability Functions Subgroup Report
 - List of BES Subsystems/BES Cyber systems Subgroup Report
 - BES Mapping Subgroup Report
 - Cyber Analysis Subgroup Report
 - Definition and Selection of Controls Subgroup Report
- 4. Subgroup Meetings (at various locations)**
- 5. Adjourn**

Friday August 21, 2009

- 1. Subgroup Meetings**
- 2. Subgroup Reports — Plenary Session**
 - Reliability Functions Subgroup Report, Q & A
 - List of BES Subsystems/BES Cyber systems Subgroup Report, Q & A
 - BES Mapping Subgroup Report, Q & A
 - Cyber Analysis Subgroup Report, Q & A

- Definition and Selection of Controls Subgroup Report, Q & A
- 3. Review and Decide on Work Plan – Review Proposed 2010 Meeting Schedule**
 - 4. Adjourn**

**Appendix # 2
 Attendees List
 August 20–21, 2009 Charlotte NC**

Attending in Person — SDT Members

1. Jeri Domingo-Brewer, Chr.	U.S. Bureau of Reclamation
2. Jim Breton	ERCOT
3. Jay S. Cribb	Information Security Analyst, Southern Company Services
4. Joe Doetzl	Manager, Information Security, Kansas City Pwr. & Light Co.
5. Sharon Edwards	Duke Energy
6. Gerald S. Freese	Director, Enterprise Info. Security America Electric Pwr.
7. Phillip Huff	Arkansas Electric Coop Corporation
8. John Lim	CISSP, Department Manager, Consolidated Edison Co. NY
9. Frank Kim	Ontario Hydro
10. Rich Kinas	Orlando Utilities Commission
11. Sharon Edwards	Duke Energy
12. Kevin B. Perry, Vice Ch.	Director Critical Infrastructure Protection, Southwest Power Pool
12. David S. Revill	Georgia Transmission Corporation
13. Kevin Sherlin	Sacramento Municipal Utility District
14. Keith Stouffer	National Institute of Standards & Technology
15. John D. Varnell	Technology Director, Tenaska Power Services Co.
16. William Winters	Arizona Public Service, Inc.
1. Roger Lampilla	NERC
3. Joe Bucciero	NERC/Bucciero Assoc.
6. Robert Jones	FSU/FCRC Consensus Center (Wed. & Thursday)
7. Stuart Langton	FSU/FCRC Consensus Center

SDT Members Attending via WebEx and Phone

1. Rob Antonishen	Ontario Power Generation (Friday)
2. Jonathan Stanford	Bonneville Power Administration

SDT Members Unable to Attend

1. Jackie Collett	Manitoba Hydro
2. David Norton	Entergy
3. Christopher A. Peters	ICF International
4. Scott Rosenberger	Luminant Energy

Others Attending in Person

Sam Merrill	CERT/SEI
Michael Toecker	BMcD
Peter Schneider	Subnet Solutions

Others Attending via WebEx and Phone

James Bassett	Lafayette
Mike Fischette	Lancing BWI

Matt Greek	
Rob Hardiman	
Doug Johnson	ConEd
Kim Long	Duke
Mike Mertz	SCE
Hoang Ngo	RI Eng
Nitin Patel	
Brian Smith	EnerNex
Robin Siewart	EON
Peter Schneider	

**Appendix # 3 — Meeting Evaluation Feedback Summary
August 20–21, 2009, Charlotte, NC
Meeting Evaluation Feedback for Inclusion in Facilitator’s Report**

Members used the following 0 to 10 scale in evaluating the meeting: 0 means totally disagree and 10 means totally agree.

1. Please assess the overall meeting.

7.78 The agenda packet was very useful.

6.83 The WebEx document display and the audio were effective

8.50 The quality of the meeting facility was good.

7.40 The objectives for the meeting were stated at the outset.

8.30 Overall, the objectives of the meeting were fully achieved.

Was each of the following meeting objectives fully achieved:

7.90 Review the work plan going forward and assess “Version 2.5” possibilities.

8.10 Receive MRC presentation and Leadership Coordination Meeting summary.

7.13 Receive updates on TFE, VSL/VRF and related cyber security efforts;

8.50 Receive and discuss reports from CIP 002 Subgroups identifying key issues and coordination points;

9.00 Convene CIP 002 Subgroup meetings;

9.20 Receive and discuss Subgroup reports on progress made; and

8.80 Agree on Work plan, next steps and assignments

2. Please tell us how well you believe the Team engaged in the meeting.

8.70 The Chair and Vice Chair provided leadership and direction to Team and Facilitators

9.20 The Facilitators made sure the concerns of all members were heard.

8.30 The Facilitators helped clarify and summarize issues.

7.63 The Facilitators helped members build consensus.

9.10 The Facilitators made sure the concerns of all participants were heard.

8.10 The Facilitators helped us arrange our time well.

3. What is your level of satisfaction with what was achieved at the meeting?

8.11 Overall, I am very satisfied with the results of the meeting.

8.13 Overall, the design of the meeting agenda was effective.

8.22 I was very satisfied with the services provided by the Facilitators.

7.89 I am satisfied with the outcome of the meeting.

7.25 I am satisfied with the progress we are making as a Team.

8.75 I know what the next steps following this meeting will be.

8.75 I know who is responsible for the next steps.

See other side

4. Other comments (use other side)

- Small groups good!
- I'd like the sub-teams to do most work offline rather than taking most of our time in sub-team meetings. We need more time together as a group reviewing each other's work and integrating it.
- The inclusion of additional personnel with operating experience was helpful.
- No space on the other side! Until everyone sees responses from the paper we are doing make-work. I believe our over all direction will change when we see the replays. I am a lemming running over the cliff because the facilitators don't know the subject and history. Jerry, Kevin, Jon D, Philip only know normal IT processes.

What did we achieve?

- Make work
- Concrete work on CIP 002

What are our biggest challenges going forward?

- Finishing the amount of work within time parameters.
- Teaching history.
- A coherent/consistent and clear CIP 002.

What suggestions do you have for making our group more productive?

- Sub-team meetings are difficult without projectors.
- Much work is being done in sub-team Silos. This approach created some of the issues with CIP v1. More coordination is required among the various teams to ensure all issues are addressed but NOT addressed by multiple teams.

Appendix # 4 — NERC Antitrust Compliance Guidelines

I. General

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

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

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

II. Prohibited Activities

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

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

III. Activities That Are Permitted

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

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

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

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

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

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

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

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

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

APPENDIX # 5
Meeting Schedule
October 2008–December 2010

Development of CIP Version 2 and Version 3 Framework
October 2008–July 2009

- 1. October 6–7, 2008 — Gaithersburg, MD** Reviewed CIP-002-CIP-009, Agreed on Version 2 approach.
- 2. October 20–21 — Sacramento, CA** CIP-002-CIP-009 Version 2 development
- 3. November 12–14, 2008 — Little Rock, AR** CIP-002-CIP-009 Version 2 adoption for comment and balloting; CIP-002-CIP-009 Version 3 process reviewed.
- 4. December 4–5, 2008 — Washington D.C.** CIP-002-CIP-009 Version 3 reviewed and debated, SDT member white papers assigned.
- 5. January 7–9 — Phoenix, AZ,** Reviewed Technical Feasibility Exceptions white paper, reviewed industry comments on CIP-002-CIP-009 Version 2 products — established small groups to draft responses, reviewed Version 3 white papers.
January 15 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
January 21 — WebEx meeting(s) Small group drafted responses to industry Version 2 comments.
- 6. February 2–4, 2009 — Phoenix, AZ** Update on NERC Technical Feasibility Exceptions process, VSL process and SDT role, review of Version 3 White papers, strawman and principles, reviewed and adopted SDT responses to industry comments on Version 2 and Version 2 Product Revisions.
- 7. February 18–19, 2009 — Fairfax, VA** Update on Version 2 process, NERC TFE process and VSL Team process; reviewed, discussed and refined Version 3 CIP-002 White papers, strawman, and principles.
- 8. March 10–11, 2009 — Orlando, FL** Update on NERC TFE and VSL and VRF Team process and review and refine Version 3 CIP-002 Strawman Proposals
March 2–April 1, 2009 — 30-day Pre Ballot
Mid-March — NERC posts TFE draft Rules of Procedure for industry comment
March 30, 2009 — WebEx meeting(s) White Paper Drafting Team
- April 1–10 — NERC Balloting on Version 2 Products**
April 6, 2009 — WebEx meeting — White Paper Drafting Team
April 8, 2009 — WebEx meeting(s) — White Paper Preview- Full SDT Conference Call
April 11, 2009 — Version 2 Ballot Results (Quorum: 91.90% Approval: 84.06%) and Industry Comments-
- 9. April 14–16, 2009 — Charlotte NC** Update on NERC TFE process, VSL Team process and NERC Critical Assets Survey; agreed and adopted responses for Version 2 industry comments for recirculation ballot; reviewed and refined Version 3 whitepaper and consensus points and progress report to NERC Member Representative Committee (MRC) May meeting.
April 28 and May 6, 2009 — White Paper Drafting Team Meetings and WebEx
April 17–27, 2009 — Recirculation Results: Quorum: 94.37% Approval: 88.32%
May 5, 2009 — NERC MRC Meeting, Arlington, VA- SDT progress report.
- 10. May 13–14, 2009 — Boulder City NV** Reviewed MRC presentation and further SDT refinement and discussion of the Version 3 White Paper.
June 8 and June 15, 2009 — Working Paper Drafting Team Meetings and WebEx
- 11. June 17–18, 2009 — Portland OR** Further SDT refinement of the draft CIP Version 3 Working Paper(s), reviewed SDT development process for June-December 2009; discussed potential SDT subcommittee structure and deliverables.
June — WebEx meeting(s)
 - Working Paper drafting group sessions including inputs from selected industry personnel to help establish BES categorization criteria

CIP-002 Development of Requirements, Measures, Etc. July-December 2009

12. July 13–14, 2009 in Vancouver, B.C., Canada

- SDT plenary session to review, refine, and adopt SDT Working Paper
- Adopt SDT response to NERC for Interpretation of CIP-006-1
- Review and adopt proposal for CIP-002 Subgroups and Deliverables
- Convene Subgroup organizational meetings to develop work plans
- Adopt 2010 Meeting Schedule

July–August Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting (as needed)

August 3–5, 2009 in Winnipeg, Manitoba **NERC Member Representative Committee**

Progress Report and presentation on new CIP Version 3 Working Paper-Concept- Reliability Standards on Cyber Security for MRC input.

13. August 20–21, 2009 in Charlotte, NC

- SDT Plenary session to review and respond to MRC input on Working Paper/CIP-002 Concepts
- SDT Subgroup and plenary meetings to develop CIP-002 requirements and “proof of concept” control (s).

July–September — 45-day Industry Comment Period on CIP-002 Concept Working Paper

NERC Webinar

August–September Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

14. September 9–10, 2009 in Folsom, CA

- SDT plenary session to review and respond to any additional industry comments on Working Paper and CIP-002 Concepts
- SDT Subgroup drafting meetings- consider industry comments, draft requirements and “proof of concept” control (s).
- SDT plenary session(s) Subgroup reports on requirements
- Review of CIP-002 Standards, Requirements, Measures, and Outline
- Address coordinating issues.
- Establish SDT meeting dates and proposed locations for January–December 2010

September–October Interim WebEx meeting(s)

- CIP-002 Subgroup meetings (as needed)
- CIP-002 Coordination Team meeting

15. October 20–22, 2009 in Kansas City, MI

- SDT Subgroup drafting meetings — day one
- SDT Plenary Session(s) — day two Subgroup reports on CIP-002 requirements
- Review and refine initial draft of CIP-002 single text

October–November Interim WebEx meeting(s)

- CIP-002 Coordination Team meeting

16. November 17–19, 2009 in Orlando, FL

- SDT plenary session(s) — to review and refine CIP-002 standard, requirements, measures and controls.

November–December Interim WebEx meeting(s)

- Drafting teams as needed to finalize drafts
- CIP-002 Coordination Team meeting

17. December 15–16, 2009 in Little Rock AK

- SDT plenary session(s) to review, refine, and agree on and adopt CIP-002 standard, requirements, measures and controls.
- Agree on initial posting of draft CIP-002 for industry review and comment.

**Refinement of CIP-002 and Development of Other CIP Standards
 January–December 2010**

(12 SDT monthly meetings and Subgroup WebEx meetings as needed)

- SDT responds to industry comments on initial and subsequent postings of CIP-002, Version 3 (may be multiple comment periods, as required)
- Refine the CIP-002 through the comment period and submit new CIP-002 Version 3 Standard for Balloting along with the catalogue of controls (i.e. CIP-003-CIP-009 or its successor) OR
- Ballot CIP-002 while permitting industry to rely on CIP 003-CIP-009 until the full suite of controls (i.e. CIP-003-CIP-009 or its successor) is reviewed and presented for balloting.
- Submit the full suite of CIP Reliability Standards on Cyber Security for Industry Comment
- Refine and Submit the full suite of CIP standards for industry ballot
- NERC Board of Trustees adoption of the full suite of standards
- FERC approves and NERC Implements the full suite of CIP standards

Proposed 2010 Meeting Schedule

18. January 20–21 — Wednesday–Thursday, Atlanta GA	24. July 14–15, Wednesday–Thursday
19. February 18–19 — Thursday –Friday, Austin TX	25. August 11–12, Wednesday–Thursday
20. March 9–11 — Tuesday–Thursday, Phoenix, AZ	26. September 8–9, Wednesday–Thursday
21. April 14–15 — Wednesday–Thursday, Atlanta GA	27. Oct. 13–14, Wednesday–Thursday or Oct.12–14
22. May 12–13 — Wednesday–Thursday, Dallas TX	28. November 17–18, Wednesday–Thursday
23. June 9–10 — Wednesday–Thursday, Sacramento CA	29. December 15–16, Wednesday–Thursday

Appendix # 6

Technical Feasibility Exceptions Matrix of Applicable Requirements

CIP-002-1/R1	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	No exceptions
CIP-002-1/R1.1	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	No exceptions
CIP-002-1/R1.2	The risk-based assessment shall consider the following assets: <ul style="list-style-type: none"> • Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard. • Transmission substations that support the reliable operation of the Bulk Electric System. • Generation resources that support the reliable operation of the Bulk Electric System. • Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. • Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. • Special Protection Systems that support the reliable operation of the Bulk Electric System. • Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment. 	No exceptions
CIP-002-1/R2	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	No exceptions
CIP-002-1/R3	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics: <ul style="list-style-type: none"> • The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or, • The Cyber Asset uses a routable protocol within a control center; or, • The Cyber Asset is dial-up accessible. 	No exceptions

CIP-002-1/R4	Annual Approval — A senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	No exceptions
CIP-003-1/R1	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	No exceptions
CIP-003-1/R1.1	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	No exceptions
CIP-003-1/R1.2	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	No exceptions
CIP-003-1/R1.3	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	No exceptions
CIP-003-1/R2	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	No exceptions
CIP-003-1/R2.1	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	No exceptions
CIP-003-1/R2.2	Changes to the senior manager must be documented within thirty calendar days of the effective date.	No exceptions
CIP-003-1/R2.3	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	No exceptions
CIP-003-1/R3	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	No exceptions
CIP-003-1/R3.1	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	No exceptions
CIP-003-1/R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	No exceptions
CIP-003-1/R3.3	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	No exceptions
CIP-003-1/R4	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	No exceptions
CIP-003-1/R4.1	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and	No exceptions

	security configuration information.	
CIP-003-1/R4.2	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	No exceptions
CIP-003-1/R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	No exceptions
CIP-003-1/R5	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	No exceptions
CIP-003-1/R5.1	Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	No exceptions
CIP-003-1/R5.1.1	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	No exceptions
CIP-003-1/R5.1.2	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	No exceptions
CIP-003-1/R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities.	No exceptions
CIP-003-1/R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	No exceptions
CIP-003-1/R6	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	No exceptions
CIP-004-1/R1	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: <ul style="list-style-type: none"> • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.). 	No exceptions
CIP-004-1/R2	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	No exceptions
CIP-004-1/R2.1	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	No exceptions

CIP-004-1/R2.2	<p>Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:</p> <ul style="list-style-type: none"> • The proper use of Critical Cyber Assets; • Physical and electronic access controls to Critical Cyber Assets; • The proper handling of Critical Cyber Asset information; and, • Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. 	No exceptions
CIP-004-1/R2.3	Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	No exceptions
CIP-004-1/R3	<p>Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:</p>	<p>Exception permitted for statutory restrictions.</p> <p>Exception permitted for collective bargaining agreement if entity can demonstrate good faith effort to negotiate this requirement into the contract.</p>
CIP-004-1/R3.1	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	<p>Exception inherited from CIP-004-1/R3 criteria.</p> <p>No exception required for more detailed background check – optional component of the requirement.</p>
CIP-004-1/R3.2	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	Exception inherited from CIP-004-1/R3 criteria.
CIP-004-1/R3.3	Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.	Exception inherited from CIP-004-1/R3 criteria.
CIP-004-1/R4	<p>Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.</p>	No exceptions
CIP-004-1/R4.1	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber	No exceptions.

	Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	
CIP-004-1/R4.2	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	No exceptions.
CIP-005-1/R1	Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	Exceptions inherited from CIP-005-1/R1.5 criteria. Note exemption (see CIP-005-1/R1.2 and explanatory information in the FAQ) for a Critical Cyber Asset that does not use a routable protocol and is only dial-up accessible.
CIP-005-1/R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	No exceptions.
CIP-005-1/R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.	No exceptions.
CIP-005-1/R1.5	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	Exception criteria inherited from the referenced requirements that the applicable Cyber Assets are subject to.
CIP-005-1/R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	No exceptions.
CIP-005-1/R2	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R2.1	These processes and mechanisms shall use an access control model that denies	Exception permitted where access control

	access by default, such that explicit access permissions must be specified.	rule set does not provide for “deny by default.”
CIP-005-1/R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	Exception permitted where ports and services cannot be configured.
CIP-005-1/R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	No exceptions.
CIP-005-1/R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	Exception permitted for technical infeasibility.
CIP-005-1/R2.5	The required documentation shall, at least, identify and describe: <ul style="list-style-type: none"> • The processes for access request and authorization. • The authentication methods. • The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4. • The controls used to secure dial-up accessible connections. 	No exceptions.
CIP-005-1/R2.6	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	Exception permitted for technical infeasibility.
CIP-005-1/R3	Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	Exceptions permitted for technical infeasibility of sub requirements R3.1 and/or R3.2 only.
CIP-005-1/R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	Exception permitted for technical infeasibility.
CIP-005-1/R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	Exception permitted for technical infeasibility.
CIP-005-1/R4	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	Exceptions inherited from CIP-005-1/R4.2 and R4.3 criteria.
CIP-005-1/R4.1	A document identifying the vulnerability assessment process;	No exceptions.
CIP-005-1/R4.2	A review to verify that only ports and services required for operations at these access points are enabled;	Exception inherited from CIP-005-1/R2.2.

CIP-005-1/R4.3	The discovery of all access points to the Electronic Security Perimeter;	Exception permitted if the only means to discover all ESP access points is an active scan of the network segment and such a scan would put the Critical Cyber Assets at risk.
CIP-005-1/R4.4	A review of controls for default accounts, passwords, and network management community strings; and,	No exceptions.
CIP-005-1/R4.5	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	No exceptions.
CIP-005-1/R5	Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.	No exceptions.
CIP-005-1/R5.1	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	No exceptions.
CIP-005-1/R5.2	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	No exceptions.
CIP-005-1/R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	Exception permitted if logs cannot be offloaded from the logging device, there is no alternative to the logging device, and the device cannot retain logs for the prescribed period of time.
CIP-006-1/R1	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	Exceptions inherited from CIP-006-1/R1.1 and R1.8 criteria.
CIP-006-1/R1.1	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed (“six-wall”) border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.	Exception permitted when completely enclosed (“six wall”) border cannot be established and alternative protective measures are implemented. Complete exception from the requirement is not permitted.
CIP-006-1/R1.2	Processes to identify all access points through each Physical Security Perimeter	No exceptions.

	and measures to control entry at those access points.	
CIP-006-1/R1.3	Processes, tools, and procedures to monitor physical access to the perimeter(s).	No exceptions.
CIP-006-1/R1.4	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	No exceptions.
CIP-006-1/R1.5	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	No exceptions.
CIP-006-1/R1.6	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	No exceptions.
CIP-006-1/R1.7	Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.	No exceptions.
CIP-006-1/R1.8	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	Exception criteria inherited from the referenced requirements that the applicable Cyber Assets are subject to.
CIP-006-1/R1.9	Process for ensuring that the physical security plan is reviewed at least annually.	No exceptions.
CIP-006-1/R2	<p>Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:</p> <ul style="list-style-type: none"> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets. 	No exceptions.
CIP-006-1/R3	<p>Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:</p> <ul style="list-style-type: none"> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access 	No exceptions.

	points by authorized personnel as specified in Requirement R2.3.	
CIP-006-1/R4	<p>Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:</p> <ul style="list-style-type: none"> • Computerized Logging: Electronic logs produced by the Responsible Entity’s selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3. 	No exceptions.
CIP-006-1/R5	Access Log Retention — The responsible entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.	No exceptions.
CIP-006-1/R6	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	No exceptions.
CIP-006-1/R6.1	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	No exceptions.
CIP-006-1/R6.2	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	No exceptions.
CIP-006-1/R6.3	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	No exceptions.
CIP-007-1/R1	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	Exception permitted for technical infeasibility if no offline testing environment can be established. Offline test environments can include stand-by production and DR systems as well as more traditional test environments. Typically, the permitted exception will be limited to plant and possibly substation control systems. Network management environments (switches, firewalls, domain controllers)

		might also qualify for an exception.
CIP-007-1/R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	No exceptions.
CIP-007-1/R1.2	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	Exception permitted to the extent the production environment cannot be replicated. See CIP-007-1/R1 exception comments.
CIP-007-1/R1.3	The Responsible Entity shall document test results.	No exceptions.
CIP-007-1/R2	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.1	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.2	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	Exception permitted where ports and services cannot be configured.
CIP-007-1/R2.3	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	No exceptions.
CIP-007-1/R3	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	No exception
CIP-007-1/R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	No exceptions.
CIP-007-1/R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Exception permitted when security patch cannot be implemented for technical reasons. Compensating measures MUST be applied per the requirement. The exception only applies to the inability to apply

		the security patch itself. Note, need to consider the case where the system vendor declines to support the system if unapproved patches are installed. Is this a valid reason for a TFE?
CIP-007-1/R4	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	Exception permitted for technical infeasibility.
CIP-007-1/R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.	Exception permitted for technical infeasibility.
CIP-007-1/R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	Exceptions inherited from CIP-007-1/R4.1 criteria.
CIP-007-1/R5	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	No exception.
CIP-007-1/R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	No exception.
CIP-007-1/R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	No exception.
CIP-007-1/R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	No exceptions.
CIP-007-1/R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	No exceptions.
CIP-007-1/R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	No exceptions.
CIP-007-1/R5.2.1	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	No exceptions.
CIP-007-1/R5.2.2	The Responsible Entity shall identify those individuals with access to shared accounts.	No exceptions.
CIP-007-1/R5.2.3	Where such accounts must be shared, the Responsible Entity shall have a policy	No exceptions.

	for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	
CIP-007-1/R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	Exceptions inherited from CIP-007-1/R5.3.1 and R5.3.2 criteria.
CIP-007-1/R5.3.1	Each password shall be a minimum of six characters.	Exception permitted for technical infeasibility.
CIP-007-1/R5.3.2	Each password shall consist of a combination of alpha, numeric, and “special” characters.	Exception permitted for technical infeasibility.
CIP-007-1/R5.3.3	Each password shall be changed at least annually, or more frequently based on risk.	No exception.
CIP-007-1/R6	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	Exceptions inherited from CIP-007-1/R6.3 and R6.4 criteria.
CIP-007-1/R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	No exceptions.
CIP-007-1/R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	No exception.
CIP-007-1/R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.	Exception permitted for technical infeasibility.
CIP-007-1/R6.4	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	Exception inherited from CIP-007-1/R6.3 criteria.
CIP-007-1/R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	No exceptions.
CIP-007-1/R7	Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.	No exceptions.
CIP-007-1/R7.1	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	No exceptions.
CIP-007-1/R7.2	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	No exceptions.
CIP-007-1/R7.3	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	No exceptions.

CIP-007-1/R8	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	Exception inherited from CIP-007-1/R8.2 criteria.
CIP-007-1/R8.1	A document identifying the vulnerability assessment process;	No exceptions.
CIP-007-1/R8.2	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	Exception inherited from CIP-005-1/R2.2 and CIP-007-1/R2, R2.1, and R2.2.
CIP-007-1/R8.3	A review of controls for default accounts; and,	No exceptions.
CIP-007-1/R8.4	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	No exceptions.
CIP-007-1/R9	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	No exceptions.
CIP-008-1/R1	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	No exceptions.
CIP-008-1/R1.1	Procedures to characterize and classify events as reportable Cyber Security Incidents.	No exceptions.
CIP-008-1/R1.2	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	No exceptions.
CIP-008-1/R1.3	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.	No exceptions.
CIP-008-1/R1.4	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	No exceptions.
CIP-008-1/R1.5	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	No exceptions.
CIP-008-1/R1.6	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	No exceptions.
CIP-008-1/R2	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	No exceptions.
CIP-009-1/R1	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	No exceptions.
CIP-009-1/R1.1	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	No exceptions.

CIP-009-1/R1.2	Define the roles and responsibilities of responders.	No exceptions.
CIP-009-1/R2	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	No exceptions.
CIP-009-1/R3	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.	No exceptions.
CIP-009-1/R4	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	No exceptions.
CIP-009-1/R5	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	Exception permitted for technical infeasibility when there is no ability to create a suitable test environment to restore the backup information to.