NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

30th Meeting Summary
Cyber Security Order 706 SDT — Project 2008-06

Columbus, Ohio

January 18, 2011 | Tuesday - 8 a.m. to 6 p.m. EST
January 19, 2011 | Wednesday - 8 a.m. to 6 p.m. EST
January 20, 2011 | Thursday - 8 a.m. to 6 p.m. EST

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Cyber Security Order 706 SDT- Project 2008-06
30TH MEETING
January 18-20, 2011
Columbus, Ohio

EXECUTIVE SUMMARY

John Lim, Chair of the CSO 706 SDT welcomed members and other participants to Columbus and thanked Jerry Freese, Jim Fletcher and Brian Newell at American Electric Power for hosting the meeting. Howard Gugel, NERC, conducted a roll call and reviewed the antitrust and public meeting guidelines at the beginning of each day. On Tuesday morning, the SDT unanimously adopted the December 14-16, 2010 Orlando meeting summary. The chair outlined the objectives the SDT sought to accomplish by the end of the meeting that included reviewing the results of the Final Ballot for CIP Version 4, developing CIP Version 5 Need, Goals and Objectives in support of the SDT's decision to adopt the results based standards format in the development of CIP V5, reviewing the current status of CIP-010 and CIP-011, and developing a communication plan for CIP V5.

The Chair announced that the FSU consensus team would no longer be participating in SDT meetings. Robert Jones from the Florida Conflict Resolution Consortium addressed the group to express their pleasure in working with the SDT and best wishes for the project moving forward. In response, the chair expressed appreciation on behalf of the SDT for the exemplary services provided by Robert Jones, Stu Langton and Hal Beardall since the inception of this SDT and best wishes in their future endeavors.

The Chair reported to that team that four members had submitted their resignation from the SDT: Jackie Collett from Manitoba Hydro, Dave Norton from Entergy, Patricio Leon-Alvarado from Southern California Edison, and Bradley (Brad) Yeates from Southern Company. The team expressed its appreciation for the participation of these members. The Chair then asked that each member actively participate in the meetings. In particular, if a member is unable to attend a SDT meeting either in person or by phone, they are asked to inform the Chair so that any possible quorum issues can be addressed prior to the meeting. If a member consistently cannot meet team meetings, they are asked to resign from the team.

The Chair expressed appreciation for the SDT's considerable work over the last quarter of 2010 in developing an industry approved version of the CIP standards that replaced the previous risk based assessment methodology in CIP-002-3 with a bright line criteria contained in CIP-002-4. On December 31, 2010, the registered ballot body approved the version 4 set of CIP standards with a 90.49% quorum, and a 80.56 % approval rating.

Scott Mix provided an update on the recent ballot for updates to CIP-005-4 regarding remote access. The team for Project 2010-15 is continuing to develop responses to comments and modify the proposed requirement in response to comments. That team is still working toward the goal of submitting the approved revised CIP-005-4 to FERC in time for the commission to act in conjunction with the CIP-002-4 action.

Based on the decision of the team to adopt the results based standard model for the next version of the CIP standards, the team chose to spend time at this meeting developing Needs, Goals, and Objectives. After spending considerable time discussing each aspect, the team unanimously adopted the document in Appendix 3.

The team then discussed the approach to developing the standards. The merits and disadvantages concerning the sub-team approach that the team has used to date were fully vetted. The team decided to continue this approach, but has chosen not to break into sub-teams during face-to-face meetings. The current makeup of each sub-team is contained in Appendix 4. The team also had a discussion on the differences between a "CIP-003 to CIP-009" approach versus a "CIP-010 and CIP-011" approach. A document detailing that discussion is in Appendix 5. At this point the team is continuing to develop CIP-010 and CIP-011, with the understanding that they could break apart CIP-011 in the future if they choose.

On Thursday, Brian Newell provided the SDT a *Lunch and Learn* presentation on the implementation of CIP Cyber Security Standards within plant networks.

The latest meeting schedule is in Appendix 6. Further discussions were held on the communication plan, which is located in Appendix 7. The team then discussed the outstanding directives of FERC Order 706, which is located in Appendix 8. The SDT then made the following assignments:

- Philip Huff is to revise the style guide based on discussions of deliverables for the February meeting.
- Everyone is to perform a review of CIP-010.
- Each sub-team is to (1) develop/review rationale statements for each requirement in CIP-011, (2) document prior version references, (3) develop change justification for each table row, and (4) review and refine requirement language and applicability.
- Howard Gugel to reach out to Mike Moon and other NERC staff to provide input during the February meeting.
- Philip Huff is to create a CIP mapping document for the February face-to-face meeting.
- NERC staff to add interpretations and CANs to the *FERC Directives by Sub-Team* document

The Chair thanked Jerry Freese, Jim Fletcher, Brian Newell and AEP for the hosting of the SDT in Columbus.

The meeting adjourned at 4:40 on Thursday, January 20, 2011

Appendix # 1— Meeting Agenda
Project 2008-06 Cyber Security Order 706 SDT
Draft 30th Meeting Agenda
January 18, 2011 Tuesday - 8:00 AM to 6:00 PM EST
January 19, 2011 Wednesday - 8:00 AM to 6:00 PM EST
January 20, 2011 Thursday - 8:00 AM to 6:00 PM EST
American Electric Power Offices
1 Riverside Plaza, Columbus OH

NOTE: Agenda Times May be Adjusted as Needed during the Meeting

Proposed Meeting Objectives/Outcomes:

- To review the results of the Final Ballot for CIP Version 4
- To review, refine and test support for CIP Version 5 Need, Goals and Objectives
- To review and discuss integration of results based standards format into CIP V5
- To agree on next steps and assignments

Tuesday, January 18, 2011 8:00 a.m. - 6:00 p.m. EST
- Introduction, welcome -*(Morning)*
- Review results of Ballot CIP Version 4 Final Ballot, comments and next steps and schedule *(Morning)*
- NERC staff support update (*Morning*)
- Industry review: (*Morning*)
    - Cyber Attack TF and Severe Impact Resilience TF
    - CIP-005-4 Update
    - Hill Update
- CIP V5 Needs, Goals and Objectives *(Afternoon)*

Wednesday, January 19, 2011 8:00 a.m. - 6:00 p.m. EST
- CIP-010 Group Review *(Morning)*
- Controls Review (*Afternoon*)

Thursday, January 20, 2011 8:00 a.m. - 6:00 p.m. EST
- Controls Review (*Morning*)
- Drafting assignments (*Morning/Afternoon*)
- Review SDT February, 2011 Taylor, TX Meeting Agenda (*Late Afternoon)*

Appendix # 2 Attendees List
January 18-20, 2011 Columbus

Attending in Person — SDT Members and Staff

1. Jay Cribb	Southern Company Services
2.Sharon Edwards	Duke Energy
3.Gerald S. Freese	America Electric Pwr.
4. Philip Huff, Vice Chair	Arkansas Electric Coop Corporation
5. Doug Johnson	Exelon Corporation – Commonwealth Edison
6. John Lim, Chair	Consolidated Edison Co. NY
7. David Revill	Georgia Transmission Corporation
8. Scott Rosenberger	Luminant Energy
9. Kevin Sherlin	Sacramento Municipal Utility District
10. Tom Stevenson	Constellation
11. John D. Varnell	Tenaska Power Services Co.

SDT Members Attending via ReadyTalk and Phone

12. Rob Antonishen	Ontario Power Generation (Tu, Th)
13. Jim Brenton	ERCOT
14. Joe Doetzl	Kansas City Pwr. & Light Co (Wed)
15. Jeff Hoffman	U.S. Bureau of Reclamation, Denver (Tu, Wed)
16.Rich Kinas	Orlando Utilities Commission (Wed)
17. William Winters	Arizona Public Service, Inc.
Scott Mix	*NERC*
Howard Gugel	*NERC*
Robert Jones	*FSU/FCRC Consensus Center (Tu)*

SDT Members Not Participating

Jonathan Stanford	Bonneville Power Administration
Bill Gross	NEI
Keith Stouffer	National Institute of Standards & Technology
John Van Boxtel	Portland General

Others Attending in Person

Robert Preston Lloyd	Southern California Edison
Jim Fletcher	American Electric Power
Jason Marshall	Midwest ISO
Roger Fradenburgh	N&ST
Brian Newell	American Electric Power
Dave Burtrum	AECI
Kevin Koloini	AMP (Tu)
Mike Keane	FERC
Tom Alrich	Matrikon
Jim Donahue	OVEC
Steven Parker	EnergySec
Nick Lauriat	N&ST

Others Attending via Readytalk and Phone

January 18
Anna Wang, Sharla Artz, Jan Bargen, Matt Dale, Ingrid Rayo, Barry Lawson, Katie Schnider, James Julien, David Gordon, Larry Camm, Patricio Leon, Drew Kittey, Vincent Le, Annette Johnston, Joe Weiss, Maggy Powell

January 19
Anna Wang, Hewitt Stuart, Vincent Le, Larry Camm, Sharla Artz, Andres Lopez, David Gordon, Annette Johnston, Jan Bargen, Katie Schnider, Ingrid Rayo

January 20
Maggy Powell, Vincent Le, Annette Johnston, Ingrid Rayo, Anna Wang, Jan Bargen, Christine Hasha, Chuck Abell, David Gordon, Andres Lopez, Larry Camm

Appendix #3

NEED, GOALS AND OBJECTIVES – PROJECT 2008-06 - CIP CYBER SECURITY STANDARDS V5

NEED

The need for Critical Infrastructure Protection (CIP) in North America has never been more compelling or necessary than it is today. This is especially true of the electricity sector. Electric power is foundational to our social and economic fabric, acknowledged as one of the most essential and among the most targeted of all the interrelated critical infrastructure sectors.

The Bulk Electric System (BES) is a complex, interconnected collection of facilities that increasingly uses standard cyber technology to perform multiple functions essential to grid reliability. These BES Cyber Systems provide operational efficiency, intercommunications and control capability. They also represent an increased risk to reliability if not equipped with proper security controls to decrease vulnerabilities and minimize the impact of malicious cyber activity.

Cyber attacks on critical infrastructure are becoming more frequent and more sophisticated. Stuxnet is a prime example of an exploit with the potential to seriously degrade and disrupt the BES with highly malicious code introduced via a common USB interface. Other types of attacks are network or Internet-based, requiring no physical presence and potentially affecting multiple facilities simultaneously. It is clear that attack vectors are plentiful, but many exploits are preventable. The common factors in these exploits are vulnerabilities in BES Cyber Systems. The common remedy is to mitigate those vulnerabilities through application of readily available cyber security measures, which include prevention, detection, response and recovery.

In the cyber world, security is truly only as good as its weakest implementation. The need to identify BES Cyber Systems and then protect them through effective cyber security measures are critical steps in helping ensure the reliability of the BES functions they perform.

In approving Version 1 of CIP Standards CIP-002-1 through CIP-009-1, FERC issued a number of directives to the ERO. Versions 2, 3 and 4 addressed the short term standards-related and Critical Asset identification issues from these directives. There are still a number of unresolved standards-related issues in the FERC directives that must be addressed. This version is needed to address these remaining directives in FERC Order 706.

GOALS AND OBJECTIVES

- **Goal 1:** To address the remaining Requirements-related directives from all CIP related FERC orders, all approved interpretations, and CAN topics within applicable existing requirements.
  - **Objective 1.** Provide a list of each directive with a description and rationale of how each has been addressed.
  - **Objective 2.** Provide a list of approved interpretations to existing requirements with a description of how each has been addressed.
  - **Objective 3.** Provide a list of CAN topics with a description of how each has been addressed.
  - **Objective 4.** Consider established security practices (e.g. DHS, NIST) when developing requirements.
  - **Objective 5.** Incorporate the work of Project 2010-15 Urgent Action SAR.
- **Goal 2:** To develop consistent identification criteria of BES Cyber Systems and application of cyber security requirements that are appropriate for the risk presented to the BES.
  - **Objective 6**: Transition from a Critical Cyber Asset framework to a BES Cyber System framework.
  - **Objective 7.** Develop criteria to identify and categorize BES Cyber Systems, leveraging industry approved bright-line criteria in CIP-002-4.
  - **Objective 8.** Develop appropriate cyber security requirements based on categorization of BES Cyber Systems.
  - **Objective 9.** Minimize writing requirements at the device specific level, where appropriate.
- **Goal 3:** To provide guidance and context for each Standard Requirement
  - **Objective 10.** Use the Results-Based Standards format to provide rationale statements and guidance for all of the Requirements.
  - **Objective 11.** Develop measures that describe specific examples that may be used to provide acceptable evidence to meet each requirement. These examples are not all inclusive ways to provide evidence of compliance, but provide assurance that they can be used by entities to show compliance.
  - **Objective 12.** Work with NERC and regional compliance and enforcement personnel to review and refine measures.
- **Goal 4:** To leverage current stakeholder investments used for complying with existing CIP requirements.

- **Objective 13.** Map each new requirement to the requirement(s) in the prior version from which the new requirement was derived.
- **Objective 14.** Justify change in each requirement which differs from the prior version.
- **Objective 15.** Minimize changes to requirements which do not address a directive, interpretation, broad industry feedback or do not significantly improve the Standards.
- **Objective 16.** Justify any other changes (e.g. removals, format)

- **Goal 5:** To minimize technical feasibility exceptions.
  - **Objective 17.** Develop requirements at a level that does not assume the use of specific technologies.
  - **Objective 18.** Allow for technical requirements to be applied more appropriately to specific operating environments (i.e. Control Centers, Generation Facilities, and Transmission Facilities). (also maps to Goal 2)
  - **Objective 19.** Allow for technical requirements to be applied more appropriately based on connectivity characteristics. (also maps to Goal 2)
  - **Objective 20.** Ensure that the words "where technically feasible" exist in appropriate requirements.
- **Goal 6:** To develop requirements that foster a "culture of security" and due diligence in the industry to complement a "culture of compliance".
  - **Objective 21.** Work with NERC Compliance Staff to evaluate options to reduce compliance impacts such as continuous improvement processes, performance based compliance processes, or SOX-like evaluation methods.
  - **Objective 22.** Write each requirement with the end result in mind, (minimizing the use of inclusive phrases such as "every device," "all devices," etc.)
  - **Objective 23.** Minimize compliance impacts due to zero-defect requirements.
- **Goal 7:** To develop a realistic and comprehensible implementation plan for the industry.
  - **Objective 24.** Avoid per device, per requirement compliance dates**.**
  - **Objective 25.** Address complexities of having multiple versions of the CIP standards in rapid succession.
  - **Objective 26.** Consider implementation issues by setting realistic timeframes for compliance.
  - **Objective 27.** Rename and modify IPFNICCAANRE to address BES Cyber System framework.

Appendix #4 SDT Sub-Teams

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

Appendix #5

CIP-002 to -009
Vs.
CIP-010 and 011

When we use these terms in comparison to one another, it can mean several things:

1) The *organization of requirements* split into the existing 8 standards or combined into 2 standards?

   Response: A downside of two standards is the optics of the reporting of violations for the "control" standard. "Existing eight standards" might also include one or two additional new standards.

2) The *change from a 'critical asset' method* of determining the cyber systems based on the BES asset's potential impact *to a focus on the cyber systems* themselves and their direct impact? (The 'BES Cyber System' approach – this is the 'big iron vs. cyber systems argument)

   Response: The focus is on BES Cyber Systems, scoped based on reliability functions. The issue is communicating the "position" we have adopted.

3) The *expansion of scope* from just critical assets and their associated CCA's *to all BES Cyber Systems*?

   Response: Remember, this is limited to BES Cyber Systems as scoped in "CIP-010." While we generally agree that there is a baseline of controls that need to be applied to all BES Cyber Systems, it is still to be determined what these controls are that will be proposed by the team. The challenge will be to create meaningful controls that can be practically implemented and reasonably audited for all BES Cyber Systems that will gain industry and regulatory acceptance.

4) *Leave CIP-002 to -009 as is* with changes to meet the remaining 706 directives.

   Response: Changes to the standards in response to FERC directives would be major changes that might leave only the numbers and titles intact.

Appendix 6

CSO706 SDT
Meeting Schedule and Objectives (January 2011)

Development Process

- Face-to-face meetings used to review/refine the entire Standard. Full team reviews Standards to raise issues, formulate concepts to address issues, ensure consistency across sub-teams and further develop work products.
- Sub-teams meet in open web conferences in between face-to-face meetings to address issues raised by the full team.
- Full team 2 hour web conference the 2nd Thursday from 12:00a – 2:00p after every full team meeting to receive sub-team status updates and provide initial feedback.

Meeting Location	Dates	Meeting Objective
Columbus, OH AEP	01/18 to 01/20/2011	Develop Needs, Goals and Objectives. Develop project plan.
Interim	1/20 to 2/15/2011	Sub-Teams to: (1) develop/review rationale statements for each requirement in CIP-011, (2) document prior version references, (3) develop change justification for each table row, and (4) review and refine requirement language and applicability.
Web meeting	2/3/2011	Update on work from subteams (12-2pm EST)
Taylor, TX ERCOT	2/15 to 2/17/2011	Full review of Standards requirements, rationale and change justification Discussion with NERC Compliance staff on programmatic requirements
Interim	2/17 to 3/15/2011	Sub-teams complete drafting assignments and develop measures and guidance statements.
Web meeting	3/3/2011	Update on work from subteams (12-2pm EPT)
New York, NY ConEd	3/15 to 3/17/2011	Full review of Standards requirements, measures and guidance Initial discussions on implementation plan.
Interim	3/17 to 4/12/2011	Sub-teams complete drafting assignments
Web meeting	3/31/2011	Update on work from subteams (12-2pm EPT)

Meeting Location	Dates	Meeting Objective
Sacramento, CA SMUD	4/12 to 4/14/2011	Review of Standards and implementation plan NERC and Regional audit staff review
Interim	4/14 to 5/17/2011	Sub-teams complete drafting assignments Sneak peak industry webinar(s) in early May
Web meeting	5/5/2011	Update on work from subteams (12-2pm EDT)
Little Rock, AR AECC	5/17 to 5/19/2011	Review of industry feedback Include additional NERC staff to begin quality review
Interim	5/19 to 6/21/2010	Sub-teams complete drafting assignments NERC continues quality review
Portland, OR BPA	6/21 to 6/23/2011	SDT and NERC staff quality review on documents for posting
Interim	6/23 to 7/19/2011	Posting for comment Prepare for technical workshop?
TBD	7/19 to 7/21/2011	Technical Workshop?
TBD	8/23 to 8/25/2011	Respond to comments
TBD	9/20 to 9/22/2011	Respond to comments and prepare for second posting and ballot
TBD	10/25 to 10/27	Respond to comments and prepare for third posting and ballot
TBD		
TBD		

Deliverables Needed for Posting

1. CIP Cyber Security Standards
2. Implementation Plan (Not started)
3. FERC Directives Summary (Last updated for informal comment posting)
4. CIP version 4 requirements mapping and change justification (obtained from Standards)
5. Informal Comment Summary (Reside with sub-team leads)
6. Comment Form (Not started)

Appendix 7

CSO706 SDT Communication Plan - 2011

- Develop a paragraph to be appended to communication about FERC filing for Version 4 that provides information on the SDT's plan for 2011 (1/31/2011)
- Develop a powerpoint presentation/talking points that can be used by SDT members to present information on the next version of the CIP standards to regional CIPC/Standards groups. (3/31/2011)
- Develop presentations for mini industry webinars that present various topics from "CIP-011" to solicit informal feedback prior to formal posting (4/30/2011)
- Develop information that can be included in the NERC News monthly publication (monthly in 2011)
- Develop a list of opportunities to meet with industry groups during 2nd and 3rd quarter 2011.

Appendix 8

FERC Specific directives from order 706:

The following table contains the status of all issues raised in the order that were either "direct"ed, specifically in the order, or "adopt"ed from the NOPR..

Note: Given the confusion over the SDT's inclusion of the change in CIP-008 ("Testing the Cyber Security Incident response plan does not require removing a component or system from service during the test") that the commission did not "direct", even though p 687 states: "In light of the comments received, the Commission clarifies that, with respect to full operational testing under CIP-008-1, such testing need not require a responsible entity to remove any systems from service," I did not include any issue that was not actively directed for change, such as those designated "should consider" or similar.

Paragraph	Text	Phase[1]
13	NERC is directed to develop a timetable for development of the modifications to the CIP Reliability Standards and, if warranted, to develop and file with the Commission for approval, a second implementation plan.	This compliance filing; and an implementation plan is filed with each submitted version of the standards
25	we direct NERC to address revisions to the CIP Reliability Standards CIP-002-1 through CIP-009-1 considering applicable features of the NIST framework.	Version 5
47	The Commission adopts the CIP NOPR approach regarding NERC and Regional Entity compliance	Rules of Procedure

[1] Schedule phases in this column mean one or more of the following:
- "Version 2" – complete in filed version 2
- "Version 4" – complete in version 4
- "Version 5" – planned for next major version (12-18 months plus)
- "Guideline" – stand alone guidance started after corresponding requirement is determined
- "TFE Filing" – 2009 filing on TFE proposal and Appendix 4D to RoP
- "not scheduled" – beyond Version 4
- "CMEP" – part of an existing or ongoing compliance audit, self-report or other process
- "VRF Filing(s)" – one of several already-filed (or very soon to be filed in the case of Version 2) VRF and/or VSL filings

Phase may also be self-explanatory if not one of these entries

	with the CIP Reliability Standards.	statement
49	The Commission also adopts its CIP NOPR approach and concludes that reliance on the NERC registration process at this time is an appropriate means of identifying the entities that must comply with the CIP Reliability Standards	Compliance registry process
72	We adopt our proposal in the CIP NOPR that responsible entities must comply with the substance of a Requirement.	CMEP
75	we direct the ERO to develop modifications to the CIP Reliability Standards that require a responsible entity to implement plans, policies and procedure that it must develop pursuant to the CIP Reliability Standards	Version 2
86	The Commission adopts its CIP NOPR proposal and approves NERC's implementation plan and time frames for responsible entities to achieve auditable compliance.	CMEP
89	we direct the ERO to submit a work plan for Commission approval for developing and filing for approval the modifications to the CIP Reliability Standards that we are directing in this Final Rule	This compliance filing; and an implementation plan is filed with each submitted version of the standards
90	We direct the ERO, in its development of a work plan, to consider developing modifications to CIP-002-1 and the provisions regarding technical feasibility exceptions as a first priority, before developing other modifications required by the Final Rule.	TFE Filing
96	we direct the ERO to require more frequent, semiannual, self-certifications prior to the date by which full compliance is required	CMEP program and self-certifications
97	we adopt our CIP NOPR proposals that, while an	CMEP, self-

	entity should not be subject to a monetary penalty if it is unable to certify that it is on schedule, such an entity should explain to the ERO the reason it is unable to self-certify	certification process
106	the Commission adopts the CIP NOPR proposals and directs NERC to modify the CIP Reliability Standards through the Reliability Standards development process to remove the first two Terms ["reasonable business judgment," and "acceptance of risk"], and develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception	Version 2 and TFE Filing
128	the Commission directs the ERO to develop modifications to the CIP Reliability Standards that do not include this term. We note that many commenters, including NERC, agree that the reasonable business judgment language should be removed based largely on the rationale articulated by the Commission in the CIP NOPR.	Version 2
138	the Commission directs the ERO to modify the CIP Reliability Standards through its Reliability Standards development process to remove references to reasonable business judgment before compliance audits begin.	Version 2
150	The Commission, therefore, directs the ERO to remove acceptance of risk language from the CIP Reliability Standards.	Version 2
156	the Commission directs the ERO to develop through its Reliability Standards development process revised CIP Reliability Standards that eliminate references to acceptance of risk.	Version 2
178	directs the ERO to develop a set of conditions or criteria that a responsible entity must follow when relying on the technical feasibility exception contained in specific Requirements of the CIP Reliability Standards	TFE Filing
186	the Commission adopts its proposal in the CIP	TFE Filing

	NOPR that technical feasibility exceptions may be permitted if appropriate conditions are in place.	
192	the Commission adopts the CIP NOPR proposal for a three step structure to require accountability when a responsible entity relies on technical feasibility as the basis for an exception. We address mitigation and remediation in this section and direct the ERO to develop: (1) a requirement that the responsible entity must develop, document and implement a mitigation plan that achieves a comparable level of security to the Requirement; and (2) a requirement that use of the technical feasibility exception by a responsible entity must be accompanied by a remediation plan and timeline for elimination the use of the technical feasibility exception.	TFE Filing
209	The Commission thus adopts its CIP NOPR proposal that use and implementation of technical feasibility exceptions must be governed by a clear set of criteria.	TFE Filing
211	direct the ERO to include approval of the mitigation and remediation steps by the senior manager (identified pursuant to CIP-003-1) in the course of developing this framework of accountability.	TFE Filing
212	the practical considerations pointed out by a number of the comments have convinced us to adopt an approach to the issue of external oversight different from the one originally proposed.	TFE Filing
218	we direct the ERO to design and conduct an approval process through the Regional Entities and the compliance audit process.	TFE Filing
219	we direct NERC, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities that are subject to Reliability Standards as users, owners or operators of the Bulk-Power System can safeguard sensitive	TFE Filing

	information.	
220	We direct the ERO to submit an annual report to the Commission that provides a wide-area analysis regarding use of the technical feasibility exception and the effect on Bulk-Power System reliability.	TFE Filing
221	we direct the ERO to control and protect the data analysis to the extent necessary to ensure that sensitive information is not jeopardized by the act of submitting the report to the Commission.	TFE Filing
222	we direct the ERO to develop a set of criteria to provide accountability when a responsible entity relies on the technical feasibility exceptions in specific Requirements of the CIP Reliability Standards.	TFE Filing
222	We direct the ERO to develop appropriate modifications, as discussed above.	TFE Filing
233	we direct the ERO to consult with federal entities that are required to comply with both CIP Reliability Standards and NIST standards on the effectiveness of the NIST standards and on implementation issues and report these findings to the Commission.	Ongoing discussions with Drafting Team Members from USBR, BPA, NIST; Development of Version 5
253	While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance … leave to the ERO's discretion whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two.	Guideline / Version 5
254	direct the ERO to consider these commenter concerns [how to assess whether a generator or a blackstart unit is "critical" to Bulk-Power System reliability, the proper quantification of risk and frequency, facilities that are relied on to operate or shut down nuclear generating stations, and the consequences of asset failure and asset misuse by	Guideline / Version 5

	an adversary]when developing the guidance.	
255	we direct either the ERO or its designees to provide reasonable technical support to assist entities in determining whether their assets are critical to the Bulk-Power System.	Version 4
257	we direct the ERO to consider this clarification [the meaning of the phrase "used for initial system restoration," in CIP-002-1, Requirement R1.2.4] in its Reliability Standards development process.	Guideline / Version 4
272	the Commission directs the ERO, in developing the guidance discussed above regarding the identification of critical assets, to consider the designation of various types of data as a critical asset or critical cyber asset.	Guideline / Version 5
272	The Commission directs the ERO to develop guidance on the steps that would be required to apply the CIP Reliability Standards to such data and to consider whether this also covers the computer systems that produce the data.	Guideline / Version 5
282	the Commission directs the ERO, through the Reliability Standards development process, to specifically require the consideration of misuse of control centers and control systems in the determination of critical assets	Guideline / Version 5
285	we direct the ERO to consider the comment from ISA99 Team [ISA99 Team objects to the exclusion of communications links from CIP-002-1 and non-routable protocols from critical cyber assets, arguing that both are key elements of associated control systems, essential to proper operation of the critical cyber assets, and have been shown to be vulnerable – by testing and experience].	Version 5
294	The Commission adopts its CIP NOPR proposal and directs the ERO to develop, pursuant to its Reliability Standards development process, a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the	Version 2

	risk-based assessment methodology.	
294	the Commission directs the ERO to develop a modification to CIP-002-1 to explicitly require that a senior manager annually review and approve the risk-based assessment methodology.	Version 2
322	The Commission adopts its CIP NOPR proposal to direct that the ERO develop through its Reliability Standards development process a mechanism for external review and approval of critical asset lists.	Version 4 (Note: version 4 methodology obviates the need for external review)
329	the Commission directs the ERO, using its Reliability Standards development process, to develop a process of external review and approval of critical asset lists based on a regional perspective.	Version 4 (Note: version 4 methodology obviates the need for external review)
333	we direct the ERO, in developing the accountability structure for the technical feasibility exception, to include appropriate provisions to assure that governmental entities can safeguard sensitive information	TFE Filing
355	the Commission directs the ERO to provide additional guidance for the topics and processes that the required cyber security policy should address.	Guideline
376	the Commission adopts its CIP NOPR proposal and directs the ERO to clarify that the exceptions mentioned in Requirements R2.3 and R3 of CIP-003-1 do not except responsible entities from the Requirements of the CIP Reliability Standards.	Version 5
381	The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing	Version 2

	compliance with the CIP Reliability Standards	
386	The Commission adopts its CIP NOPR proposal and directs the ERO to develop modifications to Reliability Standards CIP-003-1, CIP-004-1, and/or CIP-007-1, to ensure and make clear that, when access to protected information is revoked, it is done so promptly.	Version 5
397	The Commission directs the ERO to develop modifications to Requirement R6 of CIP-003-1 to provide an express acknowledgment of the need for the change control and configuration management process to consider accidental consequences and malicious actions along with intentional changes.	Version 5 / Guideline
412	The Commission therefore directs the ERO to provide guidance, regarding the issues and concerns that a mutual distrust posture must address in order to protect a responsible entity's control system from the outside world.	Guideline
431	The Commission adopts the CIP NOPR's proposal and directs the ERO to develop a modification to CIP-004-1 that would require affected personnel to receive required training before obtaining access to critical cyber assets (rather than within 90 days of access authorization), but allowing limited exceptions, such as during emergencies, subject to documentation and mitigation.	Version 2
433	we direct the ERO to consider, in developing modifications to CIP-004-1, whether identification of core training elements would be beneficial and, if so, develop an appropriate modification to the Reliability Standard.	Version 5
434	The Commission adopts the CIP NOPR's proposal to direct the ERO to modify Requirement R2 of CIP-004-1 to clarify that cyber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting	Version 5

	the operation and control of critical cyber assets.	
435	Consistent with the CIP NOPR, the Commission directs the ERO to determine what, if any, modifications to CIP-004-1 should be made to assure that security trainers are adequately trained themselves.	Version 5
443	The Commission adopts with modifications the proposal to direct the ERO to modify Requirement R3 of CIP-004-1 to provide that newly-hired personnel and vendors should not have access to critical cyber assets prior to the satisfactory completion of a personnel risk assessment, except in specified circumstances such as an emergency.	Version 2
443	We also direct the ERO to identify the parameters of such exceptional circumstances through the Reliability Standards development process	Version 5
460	The Commission adopts the CIP NOPR proposal to direct the ERO to develop modifications to CIP-004-1 to require immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset for any reason (including disciplinary action, transfer, retirement, or termination).	Version 5
464	We also adopt our proposal to direct the ERO to modify Requirement R4 to make clear that unescorted physical access should be denied to individuals that are not identified on the authorization list, with clarification.	Version 5
473	The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP	Version 5

	Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets.	
476	we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent	Version 5
496	The Commission adopts the CIP NOPR's proposal to direct the ERO to develop a requirement that each responsible entity must implement a defensive security approach including two or more defensive measures in a defense in depth posture when constructing an electronic security perimeter	Not scheduled System Security
502	The Commission directs that a responsible entity must implement two or more distinct security measures when constructing an electronic security perimeter, the specific requirements should be developed in the Reliability Standards development process.	Not scheduled System Security
502	The Commission also directs the ERO to consider, based on the content of the modified CIP-005-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline System Security
503	The Commission is directing the ERO to revise the Reliability Standard to require two or more defensive measures.	Not scheduled System Security
511	The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies.	Version 5
525	The Commission adopts the CIP NOPR proposal to require the ERO to modify CIP-005-1 to require	Version 5

	logs to be reviewed more frequently than 90 days	
526	the Commission directs the ERO to modify CIP-005-1 through the Reliability Standards development process to require manual review of those logs without alerts in shorter than 90 day increments.	Version 5
526	The Commission directs the ERO to modify CIP-005-1 to require some manual review of logs, consistent with our discussion of log sampling below, to improve automated detection settings, even if alerts are employed on the logs.	Version 5
528	the Commission clarifies its direction with regard to reviewing logs. In directing manual log review, the Commission does not require that every log be reviewed in its entirety. Instead, the ERO could provide, through the Reliability Standards development process, clarification that a responsible entity should perform the manual review of a sampling of log entries or sorted or filtered logs.	Version 5
541	we adopt the ERO's proposal to provide for active vulnerability assessments rather than full live vulnerability assessments.	Version 5
542	the Commission adopts the ERO's recommendation of requiring active vulnerability assessments of test systems.	Version 5
544	the Commission directs the ERO to revise the Reliability Standard so that annual vulnerability assessments are sufficient, unless a significant change is made to the electronic security perimeter or defense in depth measure, rather than with every modification.	Version 5
544	we are directing the ERO to determine, through the Reliability Standards development process, what would constitute a modification that would require an active vulnerability assessment	Version 5
547	we direct the ERO to modify Requirement R4 to	Version 5

	require these representative active vulnerability assessments at least once every three years, with subsequent annual paper assessments in the intervening years	
560	the Commission directs the ERO to treat any alternative measures for Requirement R1.1 of CIP-006-1 as a technical feasibility exception to Requirement R1.1, subject to the conditions on technical feasibility exceptions.	TFE Filing / CMEP
572	The Commission adopts the CIP NOPR proposal to direct the ERO to modify this CIP Reliability Standard to state that a responsible entity must, at a minimum, implement two or more different security procedures when establishing a physical security perimeter around critical cyber assets.	Not scheduled Physical Security
575	The Commission also directs the ERO to consider, based on the content of the modified CIP-006-1, whether further guidance on this defense in depth topic should be developed in a reference document outside of the Reliability Standards.	Not scheduled / Guideline Physical Security
581	The Commission adopts the CIP NOPR proposal and directs the ERO to develop a modification to CIP-006-1 to require a responsible entity to test the physical security measures on critical cyber assets more frequently than every three years,	Version 5
597	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirements R2.3 and R3.2.	Version 2
600	Commission therefore directs the ERO to revise Requirement R3 to remove the acceptance of risk language and to impose the same conditions and reporting requirements as imposed elsewhere in the Final Rule regarding technical feasibility.	Version 2 / TFE Filing
609	We therefore direct the ERO to develop requirements addressing what constitutes a "representative system" and to modify CIP-007-1	Version 5 / Guideline

	accordingly. The Commission directs the ERO to consider providing further guidance on testing systems in a reference document.	
610	we direct the ERO to revise the Reliability Standard to require each responsible entity to document differences between testing and production environments in a manner consistent with the discussion above.	Version 5
611	the Commission cautions that certain changes to a production or test environment might make the differences between the two greater and directs the ERO to take this into account when developing guidance on when to require updated documentation to ensure that there are no significant gaps between what is tested and what is in production.	Version 5
619	The Commission adopts the CIP NOPR proposal with regard to CIP-007-1, Requirement R4. [The Commission proposed to direct the ERO to eliminate the acceptance of risk language from Requirement R4.2, and also attach the same documentation and reporting requirements to the use of technical feasibility in Requirement R4, pertaining to malicious software prevention, as elsewhere. The Commission discussed the issues of defense in depth, technical feasibility, and risk acceptance elsewhere in the CIP NOPR and applied those conclusions here. The Commission further proposed to direct the ERO to modify Requirement R4 to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means]	Version 5 / not scheduled
622	Therefore, the Commission directs the ERO to eliminate the acceptance of risk language from Requirement R4.2	Version 2
622	The Commission also directs the ERO to modify Requirement R4 to include safeguards against	Version 5 / not

	personnel introducing, either maliciously or unintentionally, viruses or malicious software to a cyber asset within the electronic security perimeter through remote access, electronic media, or other means, consistent with our discussion above	scheduled
628	The Commission continues to believe that, in general, logs should be reviewed at least weekly and therefore adopts the CIP NOPR proposal to require the ERO to modify CIP-007-1 to require logs to be reviewed more frequently than 90 days, but leaves it to the Reliability Standards development process to determine the appropriate frequency, given our clarification below, similar to our action with respect to CIP-005-1	Version 5
629	The Reliability Standards development process should decide the degree to which the revised CIP-007-1 describes acceptable log sampling. The ERO could also provide additional guidance on how to create the sampling of log entries, which could be in a reference document.	Version 5 / guideline
633	The Commission adopts the CIP NOPR proposal to direct the ERO to clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.	Version 4
635	the Commission directs the ERO to revise Requirement R7 of CIP-007-1 to clarify, consistent with this discussion, what it means to prevent unauthorized retrieval of data.	Version 4
643	The Commission adopts its proposal to direct the ERO to provide more direction on what features, functionality, and vulnerabilities the responsible entities should address when conducting the vulnerability assessments, and to revise Requirement R8.4 to require an entity-imposed timeline for completion of the already-required action plan.	Version 5 Hodge Podge

651	We direct the ERO to revise Requirement R9 to state that the changes resulting from modifications to the system or controls shall be documented quicker than 90 calendar days.	Version 2
660	The Commission adopts the CIP NOPR proposal to direct the ERO to provide guidance regarding what should be included in the term reportable incident. … we direct the ERO to develop and provide guidance on the term reportable incident.	Guideline
661	the Commission directs the ERO to develop a modification to CIP-008-1 to: (1) include language that takes into account a breach that may occur through cyber or physical means; (2) harmonize, but not necessarily limit, the meaning of the term reportable incident with other reporting mechanisms, such as DOE Form OE 417; (3) recognize that the term should not be triggered by ineffectual and untargeted attacks that proliferate on the internet; and (4) ensure that the guidance language that is developed results in a Reliability Standard that can be audited and enforced	Version 5 / Guideline
673	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 5 / Guideline
676	the Commission directs the ERO to modify CIP-008-1 to require a responsible entity to, at a minimum, notify the ESISAC and appropriate government authorities of a cyber security incident as soon as possible, but, in any event, within one hour of the event, even if it is a preliminary report.	Version 5/ Guideline
686	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-008-1, Requirement R2 to require responsible entities to maintain documentation of paper drills, full operational drills, and responses to actual incidents, all of	Version 5

	which must include lessons learned.	
686	The Commission further directs the ERO to include language in CIP-008-1 to require revisions to the incident response plan to address these lessons learned.	Version 5
694	For the reasons discussed in the CIP NOPR, the Commission adopts the proposal to direct the ERO to modify CIP-009-1 to include a specific requirement to implement a recovery plan.	Version 5
694	We further adopt the proposal to enforce this Reliability Standard such that, if an entity has the required recovery plan but does not implement it when the anticipated event or conditions occur, the entity will not be in compliance with this Reliability Standard.	Version 5
706	The Commission adopts, with clarification, the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to incorporate use of good forensic data collection practices and procedures into this CIP Reliability Standard.	Not scheduled Response & Recovery
710	Therefore, we direct the ERO to revise CIP-009-1 to require data collection, as provided in the Blackout Report.	Not scheduled Response & Recovery
725	The Commission adopts, with modifications, the CIP NOPR proposal to develop modifications to CIP-009-1 through the Reliability Standards development process to require an operational exercise once every three years (unless an actual incident occurs, in which case it may suffice), but to permit reliance on table-top exercises annually in other years.	Not scheduled Response & Recovery
731	The Commission adopts the CIP NOPR proposal to direct the ERO to modify Requirement R3 of CIP-009-1 to shorten the timeline for updating	Version 2

	recovery plans.	
739	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP- 009-1 to incorporate guidance that the backup and restoration processes and procedures required by Requirement R4 should include, at least with regard to significant changes made to the operational control system, verification that they are operational before the backups are stored or relied upon for recovery purposes	Version 5
748	The Commission adopts the CIP NOPR proposal to direct the ERO to modify CIP-009-1 to provide direction that backup practices include regular procedures to ensure verification that backups are successful and backup failures are addressed, so that backups are available for future use.	Version 5
757	Therefore, we will not allow NERC to reconsider the Violation Risk Factor designations in this instance but, rather, direct below that NERC make specific modifications to its designations.	VRF Filing(s)
759	Consistent with the Violation Risk Factor Order, the Commission directs NERC to submit a complete Violation Risk Factor matrix encompassing each Commission approved CIP Reliability Standard.	VRF Filing(s)
767	The Commission adopts the CIP NOPR proposal to direct the ERO to revise 43 Violation Risk Factors.	VRF Filing(s)