NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minutes
Cyber Security Order 706 SDT — Project 2008-06

May 27, 2010
FERC Office
Washington, DC

Atmosphere was cordial and professional, and the meeting was constructive.

FERC staff agreed that the approach taken in the draft CIP-010 and CIP-011 standards could work, but acknowledged that a lot of work is still needed in clearly defining the requirements, tables, and Attachment II of CIP-010.

FERC staff expressed concern that the Low impact level requirements are insufficient and need to be bolstered. The Low baseline is too low.

The proposed 36-month review of the categorization needs to be shortened, at least for the first review cycle (possibly to 12 months)

Beware of hidden requirements in the purpose statements of the requirements, and review with the intent to minimize the adjectives used in the text (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability.

The bright line thresholds stated in Attachment II need to be justified or at least explained.

The SDT must ensure that all of the requirements are auditable.

Concern was expressed on the deferring of some FERC directives until next year.

FERC staff recognizes that the schedule of the project is ambitious, and appreciates the monumental effort being performed by the SDT in creating these standards.

Introductions and Anti-Trust Guidelines

Regis Binder, FERC, welcomed the NERC SDT members, industry stakeholders, and other participants to the meeting and covered meeting logistics. Joe Bucciero conducted a roll call of members and participants in the room and on the conference call, and reviewed the need to comply with NERC's Antitrust Guidelines.

John Lim, SDT Chair, thanked FERC for hosting the meeting and providing the meeting room and facilities. He also reviewed the proposed meeting agenda.

FERC staff stated that they are not speaking for the Commission, and they recognize the importance of the cyber security issues to the industry and the country. FERC staff recognized the magnitude of the herculean effort and the excellent hard work being done by the SDT, in addition to everyone's day jobs, and stated this effort was fully appreciated.

The proposed agenda for the meeting is included as an attachment to this meeting summary. FERC staff was encouraged to ask questions throughout the presentation/discussion offered by the SDT regarding the new draft CIP standards.

Review of CIP-010-1

John Lim reviewed the strategy, approach, and history of CIP-010-1. The primary objectives of this standard are to: (1) help scope the electric system assets that are within the purview of the CIP-010 and CIP-011 standards; and (2) establish a list of reliability functions and "bright-lines" for categorization of the BES cyber systems.

a. Discussion of Scope

The process and criteria currently being used today for identifying critical assets in the electric system are thought to be inadequate. For example, less than 5% of the existing generation facilities around the country are considered to be critical assets, so the SDT has identified a new approach in the new CIP-010-1 standard.
The scoping process in the existing CIP-002 standard calls for identification of critical bulk electric system assets, then the associated critical cyber assets. In CIP-010, there are no 'out of scope' bulk electric system assets; instead a categorized list of those assets and their related cyber systems is required. That is one of the major differences between CIP-002 and CIP-010.

Attachment I of the draft CIP-010 standard is meant to provide the definition of scope and applicability. CIP-010 requires the categorization of cyber systems by defining a list of the real-time reliability functions that could have an impact on the reliable operation of the bulk electric system, and if a cyber system is doing any of those functions, then it is within scope.

Categorization of the electric system assets and the cyber systems based on multiple levels (High/Medium/Low) of their potential impact on the reliable operation of the bulk electric system is key aspect of the new draft CIP-010 & CIP-011 standards. Attachment II of the draft CIP-010 standard is meant to provide the criteria or "bright lines" to identify the potential impact (High/Medium/Low) on the reliable operation of the bulk electric system if the electric system asset or its cyber systems are destroyed, degraded, misused, or otherwise rendered unavailable. The concept is to take a more holistic view and move away from consideration of individual critical cyber asset issues, and place more focus on 'system' impacts.

One of the significant concepts behind collapsing the CIP-003 to CIP-009 standards into a single standard was to clarify the requirements for audit purposes and reduce the incumbent paper work thereby providing focus on the security of the key cyber systems. The SDT is concerned about the auditability of the requirements, and wants to ensure that the CIP-010 and CIP-011 requirements are auditable.

b. Discussion of CIP-010-1 Attachment I

The CIP-010 requirements apply to cyber systems that are relevant to real-time operations (not long term planning or systems that do engineering or marketing). The current benchmark parameter is "impactful within 15 minutes", where the 15 minutes relates to when the incident occurs. Discussion and feedback from the industry to determine if the 15 minute parameter is appropriate has been solicited through the recent informal posting and comment form for the draft CIP-010 and CIP-011 standards. FERC staff suggested that the drafting team consider adding security systems, both electronic and physical, to the list of Functions Essential to Reliable Operation, although the 15-minute rule probably shouldn't apply.

c. Discussion of Bright Lines

Question: In CIP-010 R1, the phrase "execute or enable" is used; what is meant by enable?

In some cases, a cyber system directly performs a function (as identified in Attachment I), but in other cases (e.g., data collection/aggregation or display) it is providing information to an operator or other systems to enable functions.

FERC staff observations: Once these draft CIP standards are filed, they will create a different benchmark or situation from the existing CIP standards for the industry to consider. Are we improving or not? What is the key yard stick? There seems to be a general belief that the number of assets identified to be critical to reliable operation of the BES under CIP-002 is inadequate (i.e., not enough assets being identified, less than 5% of generation). When these new draft CIP standards are filed, how can it be demonstrated that the key assets are identified? The size of unit is not the necessarily the key. What is the impact of the Contingency Reserve clause? Why is it appropriate; isn't

it similar to an N-1 analysis which the Commission rejected for applying CIP-002? Is the "medium" level of impact adequate for the number of units that can potentially fall into that category?

The intent is for the new CIP-010 standard to be comprehensive, in that all bulk electric system and cyber system assets will be covered to some level of impact. The "bright lines" are being provided to help clarify the assignment of the appropriate level of impact to each of the BES Cyber System assets. The SDT recognizes that measuring impact against what is considered 'critical' today is not good enough since today's results are not acceptable.

The SDT is looking for guidance from all industry participants with a stake in the game as to what is acceptable for the bright lines, and hoping to receive some guidance through the informal comments from the industry.

Allen Mosher: The draft CIP-010 standard is an improvement over what we have today, and we need to implement it soon. It's difficult to compare it to what we have today, because we have a different paradigm. We want to maximize our effort to identify the most critical assets and focus on the control systems. We should worry most about common use failures and wide spread loss of the bulk electric system.

Gerry Adamski: What are the criteria for identifying if an approach is adequate? What is adequate, and how do we identify it to help tweak the product? A thoughtful dialogue may be needed to better define the "bright lines" in Attachment II.
While the number of megawatts or the size of a unit can be one of the criteria used, the impact on day-to-day operations is also very important. The SDT should have a solid basis for the numbers used in Attachment II to define the "bright lines" that are used in the draft CIP-010 standard.

For example, generators, units, plants, etc. that are used intermittently, are they single or multiple control systems? The number of generation MWs connected to assets or to the control systems? If three units combined are over 2000 is it a High impact system? Are three separate control systems that are networked together a single cyber system? How does contingency analysis factor into the impact level criteria evaluation, if at all?
It might be helpful if the SDT can quantify the number of MWs of generation that would be classified as High impact using the new draft CIP-010 standard vs. today under the CIP-002 standard.A re-ordering the "bright lines" criteria identified in Attachment II should be considered, putting the control center criteria first.

FERC staff expressed concern that the requirements applicable to the Low impact criteria are not sufficient, and that the Low/Medium impact bright line is set too high.
Throughout CIP-010 there are references to quantities of MW; how were those quantities selected? Adding insight into how the values were determined (e.g., was a study done; is it from operating experience) would be very helpful. NERC indicated that many of the bright-line values came from a variety of resources available to NERC, plus active

participation and input from OC & PC members in the development of the standards. FERC does not have a magic study to use in its review and assessment of the bright lines.

d. Discussion of Guidance and Auditing

The SDT members agree that guidance is necessary for each of the requirements. There hasn't been enough time spent to-date to fully develop or flesh out guidance on each requirement. There is reason to believe not everyone knows or can identify all the key assets that auditors are concerned about, since the auditors learn something new every time they perform an audit.

Two NERC auditors have been engaged with the process of defining these new draft CIP 010 & CIP-011 standards as well as participation from the regional entities. There were many auditors involved in last week's SDT technical workshop held in Dallas, TX. The easiest standard to audit is a checklist, but that is the worst way to audit. Transparency is needed on how an entity is audited. The entity needs to know how the audit will be approached. In the filing, a summary description of what discretion is left to the entity may be helpful.

NERC will have its audit department staff review the draft CIP standards and provide comments from an auditor's perspective. Are the "bright lines" bright enough, including the concept of shared cyber systems?

e. Discussion of Compliance Review Schedule

The draft CIP-010 R3 requires at least a 36 month review cycle, since the bulk electric system doesn't change that much that often. Currently a three year process is used by the entities as a review trigger for going back to look at the standards and consider if any changes have occurred that would impact the High/Medium/Low categorizations. What are the triggering events for this review? Possibly the SDT should consider that a one to two year review cycle is needed at first, and then followed by the traditional three year cycle.

How assets are allowed to move from one category to another over time may be critical. Where should these requirements be addressed; in the audit process? Also, do we need to address assets that may be critical to a neighboring entity but may not be critical to my entity even though my entity controls the assets?

1. Review of CIP 011-1

Phil Huff provided an overview of CIP-011 and led the discussion. The overall approach by the SDT was to combine CIP-003 through CIP-009 into one standard, taking into account the FERC directives, the SDT's review of the DHS catalogue of cyber security requirements, and incorporation of those requirements that would be beneficial to the reliability of the BES.

a. Discussion of One vs. Multiple Standards

CIP-011 is presented as one standard with many parts. As such, putting all of the requirements together in one standard would tend to minimize the need to make conformance and cross-reference revisions solely because an associated CIP standard was modified.

Retaining the multiple standards approach carries with it some difficulties with synchronization of the requirements and versioning of the multiple standards. Retaining the multiple standards approach would possibly make it easier for entities to split up the CIP requirements for implementation and monitoring in a way to match the unique organization of the entities.

The SDT is divided on the issue of format for CIP-011 – formatting it in one standard communicates the standards should be seen as one. A multiple standards format makes it easier to change individual standards separately. The single standard approach would simplify the ability to incrementally change the full standard. However, implementation questions have been raised related to the substantial change it represents from the Version 3 numbering of standards and requirements.

The multiple standards approach carries the compliance issue of potentially multiple violations across multiple standards for the same identified problem. On the other hand, when violations are reported by standard, the single standard approach may result in this standard standing out in the violations report by combining so many requirements into one standard.

The SDT asked a question regarding format of the CIP-011 standard to gain some industry feedback, since the SDT itself could not reach a super majority decision on the best format approach.

b. Discussion of the Requirement Tables

A new feature in CIP-011 is how the requirements are presented, which is based on applicability/impact on the reliable operation of the BES. There are several subject areas identified in CIP-011, including: security governance and policy; personnel training, awareness, and risk assessment; physical security; electronic access control; etc. Each requirement has several characteristics identified, and each requirement is assigned to one

of the subject areas. A requirement is represented in the CIP-011 draft standard through a table that groups together all of the requirement's characteristics.

A few questions were raised by FERC staff regarding the requirements tables in CIP-011. For example, what is the intent of the 'blank' entries in a table? Are entities required to do anything? Can an entity be found in violation of a requirement if the corresponding table entry is blank? Should entities look at the rows in a table to determine compliance with the requirement?

c. Discussion of Specific Requirements and Wording

CIP-011 R1.3: What is the intent? The requirement to clearly identify a senior manager is not really stated in the requirement. The requirement is for the entities to designate a single official. How do you determine that, and when do you have to designate this individual? Nothing specifically says an entity shall designate this individual.
The training requirements seem to be scattered around the CIP-011 draft standard. Possibly a consolidation of the training requirements would be helpful. Also the choice and use of words such as 'training' vs. 'education', vs. 'credentials' needs to be reviewed for consistency of meaning. What is 'sufficient' training? Need to include a sense of frequency and magnitude around the training requirements.

Overall, the SDT needs to review the draft CIP standards with respect to the use of adjectives (e.g., sufficient, proper, adequate, etc.) and clarify what is required with respect to auditability and enforceability. For example, R5 vs. R16/R18 states "ensuring" vs. "guaranteeing". Which one is correct?

The SDT acknowledged that this draft of CIP-011 was prepared by multiple subteams within the SDT, and the multiple teams did not always use consistent language in developing the requirements. The SDT has been focused on developing compliance elements, but is now focused on writing the requirements clearly while also minimizing the need for TFEs.

d. Form and Format Issues

The Enforcement office at NERC is looking at the draft CIP standards with respect to the needs for enforceability and compliance, as well as the table structure of requirements. CIP 011 covers the requirements previously included in CIP-003 thru 009; have these requirements been incorporated or do the requirements from CIP-003 thru CIP-009 need to be maintained?

Some of the more document-focused requirements are no longer in the new draft standards. Does that meet the equally protective criteria? The intent is to improve the standards by removing the administrative requirements that do not improve reliability in any way.

The need for more than paper evidence of compliance may lead to actual need to demonstrate compliance. For example, current requirements call for paper demonstration rather than allow for actual demonstration of the protection system; the latter improves security. Creation of paper lists of authorized personnel is a Chinese fire drill that does not improve system security.

A mapping will be done to identify gaps in the standards that we will address in the version coming out in July for industry comment and ballot. The idea is to explain clearly why the gaps are there, and that these gaps do not affect the reliability of the BES. One of the biggest issues is the perception of a culture of compliance. Now you have multiple violations of the same standard, and from the way it would be reported today, it would stick out. NERC/FERC need to make sure this does not present a skewed view of the CIP standards.

Concern was raised about the status of the components that make-up the tables. The 'R' (for requirement) is not used for the components in the table. How does that relate to the roll-up methodology; what is and is not a requirement? What is the status of the actual wording in the parent requirement (ahead of the table), and how does it relate to the components in the table?

In Tables R4 to R9, there seems to be a general formula for the requirement, which is each responsible entity shall apply the criteria with a goal of preventing unauthorized access to BES cyber systems. However, a responsible entity that has a Low impact BES cyber system does not have an entry in the table that indicates that the entity has to address any of the subcomponents. Is that entity still subject to the requirements of R5? Similarly, if a Medium impact cyber system has in fact restricted physical access according to 5.1, but there is in fact an unauthorized access – would that be a violation of R5? The intent of the entries in the tables and the requirements needs to be clarified. How will the goal of preventing unauthorized access be accomplished on assets with Low impact, when there is no requirement defined?

e. Discussion of Applicable Time Barometer

The discussion centered around why a 15 minute time period was selected as the barometer for the impact time stated in the draft CIP-010 standard. Isn't it dependent on current system conditions? Whatever time period is chosen will it be readily evident to the entities?

How quickly can it be determined that there is an impact on the bulk electric system? When does the impact happen? Is it objective enough for an entity to determine for purposes of verifying for audits?

Is a qualifier needed for peak electric system conditions or most stressful conditions? Time of year and load conditions may impact the determination of the time used.

The draft CIP standard is written around how the set of functions impact the reliable operation of the bulk electric system; some functions have more immediate impacts and others take longer to impact the BES.

Misuse of a system may have a longer lead time, far longer than fifteen minutes, but an equally devastating impact. The SDT might need to revisit the definition or application of the fifteen minute time period.

2. Implementation Plan

Scott Mix provided a high level overview of the implementation plan concepts and issues being considered by the SDT. A subgroup has been formed to prepare the text for the Implementation Plan. They will likely start meeting during the SDT Meeting in June 2010 in Sacramento.

Scott Mix presented the slides he recently gave at the SDT Workshop in Dallas, TX. He noted that the plan is to retire CIP 002 and CIP 003-009 within a transition period as CIP-010 and CIP-011 become effective.

a. Discussion of Implementation Plan Issues

The SDT is working on relevant timetables for implementation of the draft CIP-010 and CIP-011 standards, including how to prioritize the effort in terms of importance and in terms of timing.

The SDT needs to try to identify in a general sense which assets will eventually fall into each of the High/Medium/Low impact categories and how many assets will be in each category. A significant benchmark between the CIP-002 and the CIP-010 & CIP-011 standards will be the number of assets involved, and has that number increased in size and scope.

How should the industry be incentivize to implement the new CIP-010 & CIP-011 standards, but not the Medium or Low impact controls at the expense of first focusing on the High impact assets. Possibly a 'rolling' implementation of the standards is in order. What is the impact categorization of a BES cyber system if it moves up or down an impact level? How should it be considered in the implementation plan?
The Implementation Plan subteam will also work with the nuclear folks to discuss policies and impacts vs. an implementation schedule. Two stakeholders from the nuclear industry will be part of the implementation plan subteam.

Some level of reporting to FERC on implementation plan development (including content and schedule) is encouraged. The reporting should be designed to provide review of justifications, milestones, and accountability while offering a degree of oversight.
One possible scenario for implementation plan development would be for the entities to quickly develop their lists of categorized assets, immediately followed by the

establishment of their respective implementation plan. The responsible entities should then report their implementation plans to the respective regional entity for approval. Guidance documents will be prepared by the SDT to provide a level of consistency and assistance in the development of the implementation plans. Potential conflicts between compliance deadlines and audit schedules must also be considered.

Allow entities to be compliant early especially through implementation of system upgrades that will need to be compliant later. We'll need to recognize that some entities may need additional time to do the job right while maintaining appropriate levels of oversight. For example, larger organizations may have a larger portion of assets affected by the new standards.

During the discussion, Allen Mosher suggested that a possibility to consider would be to base the implementation plan on the current mitigation plan process. The discussion of this idea continued with many including FERC staff seeing possible merit to this approach.

b. Discussion of Transition and Migration

A transition plan from the existing CIP-002 to CIP-009 requirements to the new draft CIP-010 and CIP-011 requirements is needed. Some CIP-011 requirements are a direct replacement for those in CIP-003-009 and a migration plan should be developed for those, while other requirements are new and an implementation plan is needed. Plans to guide the entity may be helpful to both the entity and the auditors. A roadmap for the transition/migration activities would help in the development of a schedule to accomplish these tasks.

The draft CIP-011 standard does not appear to provide a significant base level of protection for the low and medium impact controls. FERC staff expressed concern that the controls requirements for the "low" impact systems do not provide an adequate level of protection. The blank entries in the tables in CIP-011 might imply that there are no control requirements.

c. Discussion of Physical Controls

Physical items or locations may have protection but may not be auditable as a NERC standard, which focuses on cyber assets. For example, substations have physical protection, but how can an auditor be convinced that the physical fence or padlock was there thirty days ago.

The focus of the SDT is on cyber security. The team considered a separate SAR for physical security. The issue is not when the fence went up, but was it secured and was the lock actually locked – actually visiting remote sites to prove this might be too much.

Too much energy goes into such audits without corresponding benefit of protecting the system. An auditor might randomly select a few remote sites – because selection is random, but an entity would need to protect them all.

d. Discussion of Immediate Revocation

It's questionable if the industry can meet targets for "immediate revocation of access". Do timeframes of 72 hours work? May need a primary and secondary revocation applied to remote and/or physical access – this will also depend on the "cause" for revocation.

What does "immediate" really mean in these cases? For example, an entity may need to revoke access of an individual before letting the person go for cause. "Immediate" is not auditable, even if we set a time period. "As soon as possible" would be a better phrase or a set time period would be sufficient. If it is a planned termination, then it can be immediate because it precedes the termination. If it is part of an emergency, revocation may need a reasonable time period.

e. Discussion of Security Systems Protection

FERC staff suggested adding a fourth column to the tables in CIP-011 that would list the physical/cyber security system protection required for each asset. The intent is to apply the appropriate level of security. It was also suggested that a function be added to the table in Attachment I of CIP-010 for security/protection systems.
Security systems impact the BES. Passwords – maximize use without being prescriptive – suggested language – cut down on TFE's

f. Beyond CIP-010 and CIP-011

FERC Order 706 included some directives (e.g., defense in depth) that have not been addressed so far. The SDT felt there was too little time to accomplish these requirements and that tackling them might have derailed the process to this point.
Concern is that some of the items may have been part of the paradigm shift FERC was asking for in Order 706. How can some of these items in the order be defined, or implemented, or audited, etc.?

Implementation of an active vulnerability assessment (testing) can be contrary to reliability and security. Special care and guidelines are needed for this requirement.
The December 2010 date for filing of the new draft CIP standards for approval by FERC is not one of the Commission directives. It can become an informational filing, since it is not making law, and may be changed with FERC approval. Need to implement improvements sooner, but may not be able to resolve issues now.

The SDT is planning to file the new draft CIP-010 and CIP-011 standards by December 2010, and will start in January 2011 to look at the other remaining issues – may be a continuously moving target.

The recent SDT Technical Workshop was aimed in part at telegraphing this schedule to the industry and thereby telling them the new standards are not a completed deal. Scott Mix stated that 'Defense in depth' is implementation of guidance or guidelines for layered security, which is guidance for designing but not necessarily an auditable requirement. Concern was expressed that 'Defense in depth' was a difficult concept to define as enforceable requirements.

The SDT would benefit from a shared dialogue with FERC Staff on defense in depth and other issues about what we are trying to achieve, the overall objective, and what is needed for the industry to reach it. This dialogue would go beyond just the standards, but could also cover how you approach audits and compliance. NERC and the SDT still have to legally deal with the directives in FERC Order 706. The SDT may ask for clarification of specific parking lot issues, or maybe a separate filing on those issues should be developed.

3. Closing

The dialogue and sharing of information during this meeting was constructive and has been very useful. The FERC staff reminded us that they do not speak for the Commission. They may not agree with the statements or agreements reached. However, with continued dialogue and progress on the issues we may at least achieve a mutual understanding of the problems and concerns being addressed.

Gerry Adamski asked FERC staff about their general sense of acceptability of the body of work to date? Also, what needs more work? The approach is responsive, but as discussed earlier, there are many questions remaining, including how the impact levels will be applied. There is still a lot of work to be done to achieve the filing by the end of 2010. It is a very aggressive schedule, but there is recognition of the quality and amount of effort involved.

Meeting adjourned.