NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Summary of CIP V5 Revisions Technical Conferences

January 21, 2014 – Atlanta, GA
January 23, 2014 – Phoenix, AZ

NERC hosted two CIP Version 5 Revisions technical conferences in Atlanta (January 21) and Phoenix (January 23), both of which were also available via the web. The intent of the conferences was to engage in early dialogue regarding the four main directives in FERC Order No. 791: (1) modify or remove the Identify, Assess, and Correct (IAC) language in 17 CIP requirements; (2) develop modifications to the CIP standards to address security controls for Low Impact assets; (3) develop requirements that protect transient electronic devices; and (4) create a definition of "communication networks" and develop new or modified Reliability Standards that address the protection of communication networks.

During these day-long discussions, industry representatives were able to discuss considerations and perspectives on addressing the directives by providing informal input to the standard drafting team (SDT). The sessions also provided NERC with the opportunity to interact with industry prior to standard drafting team activity in a meaningful manner. As a result, both industry and NERC representatives came away with a better sense of what to expect from the standards development efforts during the upcoming year to meet the FERC directives.

There was excellent participation for both conferences. In Atlanta, there were 114 in-person attendees and 170 via webinar. In Phoenix, 137 attended in-person and 121 via webinar. The large turnout for both conferences allowed us to reach a wide audience and for all participants to hear varied opinions. It also underscored the interest that industry is taking in these standard development efforts.

NERC has received positive feedback on these two conferences. Most notably, participants requested that NERC conduct similar events in the future. The slides for these conferences may be accessed here.

Identify, Assess, and Correct

One of the FERC directives was to modify or remove the 17 instances of the IAC language in the CIP Version 5 standards.[1] The IAC language was originally added to the standards to address "zero tolerance" compliance concerns regarding high frequency security obligations inherent to cyber-security. While the Commission expressed support for NERC's effort to move away from a "zero tolerance" approach to compliance, they also explained that the IAC language is overly vague and lacks basic definition and guidance. The Commission stated that its preference is to remove the language but indicated NERC may propose other modifications as long as the modifications address the concerns. FERC further directed NERC to file the removal or modifications of the IAC language for approval by February 3, 2015.[2]

Regardless of the outcome to modifications, NERC remains committed to a compliance approach that moves away from "zero tolerance" and focuses on the activities that have the greatest impact on the Bulk-Power System

[1] Version 5 Critical Infrastructure Protection Reliability Standards, 145 FERC ¶ 61,160 at P 67 (2013) (FERC Order No. 791).
[2] *Id.*

reliability. The CSO 706 SDT added the IAC language to address the "zero tolerance" issues while rewarding entities with robust programs that addressed deficiencies. In light of potential removal of this language, NERC staff and the technical conference participants engaged in an open dialogue on how to address compliance issues, including a discussion of the Reliability Assurance Initiative (RAI), which had not fully matured at the time the IAC language was added to the standards in mid-2012.

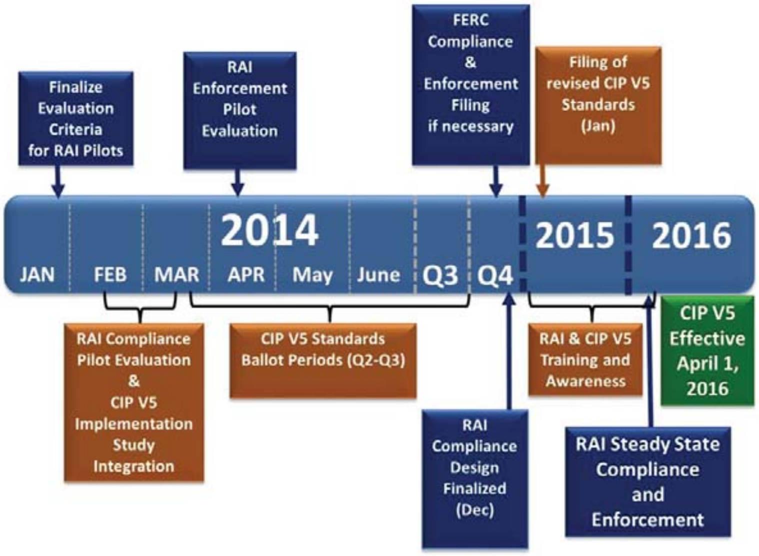
Conference attendees offered numerous considerations and comments, including the following:

- How can a modified version of the CIP Standards avoid moving back toward a zero tolerance model while addressing FERC's concerns of the IAC language, especially since industry is not aware how RAI will be implemented?

- Can the timing and balloting process for the revised standards be successful only if RAI is in a more mature state?

- The underlying issue is with the IAC language, not the concept. Will the implementation window for Version 5 allow RAI and the enforcement pilots to mirror the timelines for the drafting efforts and the maturation of RAI processes?

Following the IAC discussion, NERC staff presented information about the enforcement pilots and RAI's link to Version 5 and future standard development. Similarly, NERC staff gave an update on the CIP Version 5 Transition Study activity. The lessons learned from the Transition Study will be posted on the CIP Version 5 Training Program web site[3] and may be in scope for revisions by the SDT as appropriate.[4] Below is a timeline of all of the activities relating to CIP Version 5:


Finalize Evaluation Criteria for RAI Pilots
RAI Enforcement Pilot Evaluation
FERC Compliance & Enforcement Filing if necessary
Filing of revised CIP V5 Standards (Jan)
2014
JAN
FEB
MAR
APR
May
June
Q3
Q4
2015
2016
RAI Compliance Pilot Evaluation & CIP V5 Implementation Study Integration
CIP V5 Standards Ballot Periods (Q2-Q3)
RAI Compliance Design Finalized (Dec)
RAI & CIP V5 Training and Awareness
CIP V5 Effective April 1, 2016
RAI Steady State Compliance and Enforcement

http://www.nerc.com/pa/CI/trnstnprgrm/TransitionProgramTimeline.jpg

[3] http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx

[4] While the focus of the Standards Authorization Request (SAR) is to address the directives from FERC Order No. 791, it may be appropriate to make modifications to the CIP Version 5 standards based on the lessons learned from the Transition Study.

Low Impact Assets Protections

A key aspect of the CIP Version 5 Reliability Standards that differs from earlier versions is that they expand applicability to BES Cyber Systems that previously were not directly subject to the standards. As a result, BES Cyber Systems that are categorized as Low Impact assets must comply with CIP-003-5, Requirement R2. This requirement directs responsible entities to develop policies that address four technical areas: cyber security awareness, physical security controls, electronic access controls for external routable protocol connections and Dial-up Connectivity, and incident response to a Cyber Security Incident.

In FERC Order No. 791, the Commission stated that, "the CIP version 5 Standards, however, do not require specific controls for Low Impact assets nor do they contain clear, objective criteria from which to judge the sufficiency of the controls ultimately adopted by responsible entities for Low Impact BES Cyber Systems."[5] The Commission further stated that this "absence of objective criteria" would lead to ambiguity and result in inconsistency among entities' compliance with the requirement.[6]

Therefore, the Commission directed NERC to develop modifications to the CIP Version 5 Reliability Standards to address these concerns. In FERC Order No. 791, the Commission suggested four alternatives for addressing the directive. The Commission stated that in responding to this directive, NERC could either define a set of appropriate control objectives for Low Impact assets, define the specific controls that would apply to Low Impact assets, provide greater specificity for the processes in CIP-003-5, Requirement R2, or pursue an equally efficient and effective solution.[7]

Based on this context, the conference participants provided input for the SDT to consider when addressing the Low Impact assets directive. Among the considerations offered by conference attendees:

- Controls or criteria should be commensurate with the level of risk an asset poses.
- Entities of all sizes should be included in the development process; some entities have never had to comply with CIP Reliability Standards prior to this Version.
- Requirements should provide flexibility for entities to develop physical security controls appropriate for the level of difficulty inherent in securing open areas.
- Scalability of electronic access controls is important.
- Consider device-type and/or facility-type security measures.
- Consider the monitoring practices for some types of assets when assessing incident response plan requirements.
- Refer to Electricity Sector Information Sharing and Analysis Center (ES-ISAC) history during development.

[5] FERC Order No. 791 at P 107.
[6] *Id.* at P 108.
[7] *Id.*

- Identify requirements applicable to Low Impact assets in a requirement that is separate from those requirements that apply to Medium and High Impact assets.
- Use previous versions of CIP Standards, particularly Version 3, as reference points because many entities have already built security infrastructures based on those requirements.
- Include a desired or expected outcome within the requirements.
- Consider including the following specific controls in the requirement(s) for Low Impact BES Cyber Systems:
    - Fence height
    - Lock types
    - Entry control procedures.

Communication Networks

The CIP Version 5 Reliability Standards do not refer to communication networks within the definition of Cyber Assets. The CSO 706 SDT determined that inclusion of communication networks in that definition would lead to confusion in the implementation of Version 5 standards. The SDT stated that many components of communication networks cannot strictly comply with the Version 5 standards.

FERC noted in Order No. 791 that the Cyber Asset definition should not include communication networks.[8] However, the Commission was concerned that a gap in protection may exist becuase the CIP version 5 Standards do not address security controls needed to protect the nonprogrammable components of communication networks.[9]

As a result, FERC directed NERC to develop a definition of communication networks and develop either new or modified Reliability Standards addressing the protection of nonprogrammable components of communication networks.[10] FERC further directed NERC to file the modifications for approval by February 3, 2015.[11] NERC also notes that communications security is a topic of the FERC Staff-led conference, and the outcome of that conference may further inform the approach used to resolve this directive.

The technical conference participants offered considerations for the SDT in developing the scope of the definition and whether a new or modified standard would best address the directive. The attendees provided the following input for the SDT's consideration:

- Include a risk assessment of specific access points rather than only looking within a perimeter.
- Use a threat-based approach in identifying risk.
- Determine whether entities have control over particular aspects of a network (i.e., vendors may control certain segments).

[8] *Id.* at P 148.
[9] *Id.* at P 149.
[10] *Id.* at P 150.
[11] *Id.*

- When defining communication networks, determine what could be considered part of BES Cyber Systems so there is no overlap.
- Draft language in requirements in a manner to survive changes in technology.
- Balance adequate protections with exclusions of assets that should not be in the definition.
- First determine what needs to be protected, then consider the definition and protections in requirements.
- Keep NERC's jurisdictional restrictions in mind.
- Draw upon the expertise of communications professionals when drafting the definition.
- Consider whether the directives pertaining to communication networks should be a standard outside the CIP suite of standards.
- Consider the demarcation point as a critical component of the definition.
- Consider physical versus logical protections.
- Be aware of the potential impact of the definition and requirements on entities of all sizes.

Transient Devices

The CIP Version 5 Reliability Standards definition of BES Cyber Asset provides an exemption for a Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

In FERC Order No. 791, the Commission stated that it "remain[s] concerned whether the CIP version 5 Standards provide adequately robust protection from the risk posed by transient devices."[12] The Commission further "expects NERC to consider the following security elements when designing a Reliability Standard for transient devices or removable media: (1) device authorization as it relates to users and locations; (2) software authorization; (3) security patch management; (4) malware prevention; (5) detection controls for unauthorized physical access to a transient device and; (6) processes and procedures for connecting transient devices to systems at different security classification levels (i.e. High, Medium, Low Impact)."[13]

The technical conference participants offered considerations for the SDT in developing revisions to the Version 5 standards that address the directive of protecting transient devices. The attendees provided the following input for the SDT's consideration:

- Consider whether the directive is not to protect systems from transient devices, but to protect the transient devices themselves. While encryption is available, perhaps specific controls should be specified and evidence should be provided.

[12] *Id.* at P 132.
[13] *Id.* at P 136.

- Define “transient device,” and consider the following qualifications:
    - There could be specific requirements identified as applicable to them and could possibly address the directive.
    - Transient is something introduced to the environment and it needs to be protected from the environment.
    - Whatever is done, focus on what outcome might be and what controls might be needed.
    - Entities need to address what concerns might be, such as passwords, oversight, and protection of machines.
    - Based on device class type, define category and policy for temporary use.
- Establish controls appropriate for the device being connected and where the connection is occurring; there is no “one-size-fits-all” approach.
- Incorporate transient device protection mechanisms within configuration or change management requirements.
- Recognize a device’s role and location, because some devices were never designed to be secure so anti-malware tools also may not be effective.
- Do not simply focus on thumb drives; controls for other devices should not be overlooked.
- Avoid subcategorizing transient devices; technology constantly changes and new devices can hold/transfer data and possibly perform other actions.
- Do not overlook existing requirements for protecting assets, whether in the context of remote access, internal processing, or other priorities.
- Avoid restrictive requirements that will not be able to adequately address changing technology.
- Specify device protection requirements pertaining to updates that must be downloaded from vendor sites.
- Address protection mechanisms that may be implemented for BES systems from risks posed by plugging in transient devices; there are tools used to perform network analysis that could expose all vulnerabilities to anything that resides on the device.
- Determine whether the discussion of transient devices should be limited to the use of maintenance devices; earlier discussions by the CSO 706 SDT may have been unwittingly restrictive.
- Consider whether there should be controls in place to alert when something is connected to network and whether certain systems or devices are segmented. Also consider if change control processes should be part of this effort, such as a logging/monitoring client on Windows devices that automatically issues a notification when something is plugged in. Closing out unnecessary ports, change control and asset management are logical fits for these processes.
- Consider whether the DOE initiative on procurement might be appropriate to reference.

- Account for different use cases; for example: technician laptops used at multiple sites; laptops represent a greater threat than static PCAs; also consider flash drives, vendor devices, and remote access issues.
- Assess whether the one year deadline for addressing the cited issues is appropriate; there were different opinions expressed by conference attendees as to its feasibility.
- Review the current standard language to determine whether it introduces a vulnerability regarding transient devices.
- Auditability is an issue because of the lack of records.

Survey

In FERC Order No. 791, the Commission "directed NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods."[14] The Commission further expects NERC to explain "(1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition."[15]

NERC reached out to the participants to gauge options for conducting this survey as well as ideas to effectively gather the input FERC directed NERC to collect while not being overly burdensome. Participants provided their views on the different avenues NERC can take to produce the results needed for the informational filing, and NERC is working to incorporate some of the feedback in developing its survey.

Next Steps

The Standards Committee appointed the SDT on January 29, 2014. The SDT consists of ten members, including two co-chairs. The first SDT in-person meeting will be held February 19-21, 2014 at NERC's offices in Washington, D.C. If you would like to follow the SDT's development activity, please visit the project page on NERC's website here and/or send a request to Marisa Hecht or Ryan Stewart to be added to the team's "plus" email list.

[14] *Id.* at P 124.
[15] *Id.*