Revised CIP Standards Approved by FERC

Industry Petitions FERC for Expedited Action to Align Implementation Plan Dates

On January 21, 2016 FERC issued Order No. 822 approving the revised CIP version 5 (V5) standards modified by NERC and its stakeholders in response to FERC’s earlier directives.

The approved CIP standards provide for new cyber security controls and require that a greater number of utility systems be protected. Due to the complexity of the changes, NERC has been facilitating utility compliance planning through its comprehensive CIP Transition Program.

Utilities should be well underway with their implementation plans in order to be compliant with the CIP standards by the effective dates for the revised standards commencing April 2016. However the timing of the January 21 order has created an implementation plan complication for utilities as discussed further below.

Standards Approved by FERC

In its order FERC approved seven revised critical infrastructure protection (CIP) Reliability Standards:

- CIP-003-6 (Security Management Controls)
- CIP-004-6 (Personnel and Training)
- CIP-006-6 (Physical Security of BES Cyber Systems)
- CIP-007-6 (Systems Security Management)
- CIP-009-6 (Recovery Plans for BES Cyber Systems)
- CIP-010-2 (Configuration Change Management and Vulnerability Assessments)
- CIP-011-2 (Information Protection)

Additionally FERC directed NERC to develop certain modifications to improve the CIP Reliability Standards. These will be the subject of future CIP standards development efforts by NERC.

Background

On November 22, 2013, the Federal Energy Regulatory Commission (FERC) issued Order No. 791 approving NERC’s version 5 CIP standards and implementation. The Order authorized the direct transition to the new CIP version 5 standards allowing utilities to skip the interim version of the standards known as CIP Version 4.

On February 12, 2015 the NERC Board of Directors approved all proposed industry approved changes to the Critical Infrastructure Protection (CIP) Reliability Standards that are necessary to respond to the directives in the FERC final November 2013 approval order. On February 13, 2015 NERC filed the petition containing the
necessary revisions with FERC. The NERC petition presented the technical basis and purpose of the proposed Reliability Standards along with a summary of the development history.

FERC also proposed that NERC develop certain modifications to Reliability Standard CIP-006-6, including changes to require protection for communication network components and data communicated between all bulk electric system Control Centers. In addition, FERC stated that while the technical controls in proposed Reliability Standard CIP-006-6 are generally consistent with the type of controls cited in its Order No. 791, FERC was concerned that a reliability gap existed because the applicability of the proposed standard is limited to BES Cyber Assets within the same Electronic Security Perimeter. This would leave the communication systems outside the Electronic Security Perimeter vulnerable.

Order 822 is the conclusion of the process initiated on July 16, 2015 through a FERC Notice of Proposed Rulemaking (NOPR). In its NOPR FERC identified several concerns and proposed a new standards initiative regarding critical infrastructure supply chain issues. The FERC order issued on January 21 addresses all issues identified in the NOPR except for the supply chain issue\(^1\). The supply chain issue will be the subject of a separate review and order.

More information is available in TRC’s previous Regulatory Update on this topic.

**2016 Directives**

FERC has directed NERC to modify the standards to address certain reliability risk concerns as follows:

- **Transient Devices** - The adoption of controls for transient devices used at Low Impact BES Cyber Systems, including Low Impact Control Centers, will provide an important enhancement to the security posture of the bulk electric system by reinforcing the defense-in-depth nature of the CIP Reliability Standards at all impact levels. FERC directed NERC to develop mandatory protection for transient electronic devices used at Low Impact BES Cyber Systems in a manner that effectively addresses, and is appropriately tailored to address, the risk posed by those assets.

- **Communications Links** - Modifications to CIP-006-6 to provide controls to protect, at a minimum, communication links and data communicated between bulk electric system Control Centers are necessary in light of the critical role Control Center communications play in maintaining bulk electric system reliability. FERC directed NERC to enhance mandatory protection for communication links and

\(^1\) The Supply Chain issue is related to the acquisition of Operating Technology equipment to address risks to communication networks and related bulk electric system assets. The proposal would call for the development of new standards for supply chain management security controls to protect the electric system from introduction of new security vulnerabilities and malware threats. FERC conducted a Technical Conference on January 28, 2016 to gather additional information. A separate Order on this topic is expected in the future.
data communicated between bulk electric system control centers in a manner that reflects the risks posed to bulk electric system reliability.

FERC also directed NERC to conduct a study on the strength of the CIP version 5 remote access controls and the risks posed by remote access-related threats and vulnerabilities. This research may result in future changes to the CIP standards in the area of remote access methods once FERC analyzes NERC’s findings.

**Specific Transition Guidance is Available**

At the request of industry, NERC has created a number of guidance documents and has published the results of compliance trials for the new CIP standards. The materials are available on a special “Initiatives” project page for CIP Implementation. Utilities should review this material in detail as they prepare plans for the transition to the new CIP standards.

While many of the implementation issues discovered in the pilot study period were relatively straightforward, some were particularly challenging and required significant time and effort to address sufficiently. It is important to review this report and other guidance found on the NERC CIP Transition page to support your company’s compliance success.

**Future Standards Development**

A January 19, 2016 webinar announced NERC’s intent to develop changes beginning after the April 1 implementation date of the V5 standards. The new directives of Order 822 will likely be incorporated in the next CIP standards development effort along with the items previously identified in the V5 transition period. There will be an outreach effort to obtain industry input as to additional areas needing clarification. At the February 10, 2016 NERC Member Representatives Committee meeting members of NERC staff outlined the plans to develop a new standards drafting effort which will address all open issues and the new directives.

**Implementation Plan and Effective Date**

The approved CIP V5 standards are effective between April 1, 2016 and September 1, 2018 as specified in the approved Implementation Plan. Utilities must comply with the requirements applicable to Low Impact BES Cyber Systems (CIP-003-6, Requirement R1, Part 1.2 and Requirement R2) beginning April 1, 2017, consistent with NERC’s original Implementation Plan.

Order 822 also approved NERC’s proposed Implementation Plan related to the revised CIP standards listed above and as a result, the recently modified and approved CIP Reliability Standards will be effective July 1, 2016.

FERC recognized the timing concerns raised by commenters in the NOPR regarding the potential burden of implementing two versions of certain CIP Reliability Standards within a short period of time. In Order No. 822
FERC indicated it was willing to consider requests to align the implementation dates of certain CIP Reliability Standards. In response, several utility trade organizations filed a joint petition with FERC requesting that FERC grant an extension of time to defer implementation of the CIP V5 standards from April 1, 2016 to July 1, 2016 in order to align all of effective dates. Expedited action was requested.

Next Steps

The CIP standards will evolve as a result of the changing nature of the security threats. Utilities should continue to stay abreast of those changes and adapt their CIP standards compliance programs to these changing standards. TRC can help your company remain in compliance.

Resources

- CIP Approval Order No. 822 - January 21, 2016
- FERC Notice of Proposed Rulemaking - Revised
- Critical Infrastructure Protection Reliability Standards
- NERC Petition to FERC with Revised CIP Standards
- NERC Webinar on Future CIP Standards Development
- NERC CIP Transition Program Initiative Page
- NERC CIP Transition Implementation Guidance
- NERC CIP Trial Report
- TRC Transition Guidance
- TRC Security Services

About Us

TRC’s Technology Engineering team has an in-depth understanding of power generation, transmission engineering, operational technology and the latest security, building safety, and security management systems on the market. We provide a suite of communication engineering services for all utility networks. We are well versed in the regulatory documents driving infrastructure protection. Our 40 critical infrastructure protection and security staff nationwide have 30 years of experience executing design contracts, guiding clients through mitigation and implementation projects, and providing testing and commissioning services. We work with clients on forward-thinking and forward-leaning initiatives related to the physical “hardening” and cyber protection and of critical infrastructure. Our team includes former utility directors and managers experienced with the NERC standards and risk-based programs. We have the expertise needed to assess, design, oversee, implement and test the security technology for an effective cyber and physical security program.

*This regulatory update is a service to our utility clients, helping keep them informed of issues that impact their reliability risk and business goals.*

February 12, 2016