Akin®

FERC Accepts Revisions to Cybersecurity Reliability Standards, Orders Further Revisions

Jan 25, 2016

Reading Time : **6 min**

In Order No. 822, FERC accepted NERC's revisions and also ordered additional revisions to the CIP Version 5 standards. First, FERC directs NERC to make additional revisions to the CIP Version 5 standards addressing the risks posed by transient electronic devices (such as laptops, thumb drives, tablets, and a wide array of diagnostic and testing equipment) to Low Impact Bulk Electric System (BES) Cyber Assets, which include essentially all computer systems associated with the bulk electric system, except control centers, generation facilities and transmission facilities. As discussed below, in Order No. 822, the Commission has accepted revisions addressing risks to Low Impact BES Cyber Assets generally, and also approved revisions that addressed the risk of transient devices to High and Medium Impact BES Cyber Assets. However, the Commission remains concerned about risks posed to Low Impact BES Cyber Assets by transient devices, which is not addressed in the current rules. The Commission's concerns relating to transient devices and Low Impact BES Cyber Assets was first raised in the NOPR, based on a concern that malware inserted at one substation might propagate unchecked through multiple substations or a utility's other cyber assets. Although most commenters, including NERC, opposed the addition of controls for transient devices with regard to Low Impact BES Cyber Assets, FERC has concluded that such controls are necessary, since the firewalls prescribed by the current standards may not curb the spread of malicious code. One solution would be for NERC to extend the limitations on transient devices related to High and Medium Impact BES Cyber Assets to Low Impact BES Cyber Assets, but the Commission is not specifically ordering that change.

Additionally, FERC directs NERC to modify its standards relating to communications networks to require protections for communication network components and data used for intra-

Control Center communications based on the risk posed to the BES. NERC also is ordered to conduct a "comprehensive study that identifies the strength of the CIP version 5 remote access controls, the risks posed by remote access-related threats and vulnerabilities, and appropriate mitigating controls." Finally, NERC must develop modifications to its definition for "Low Impact External Routable Connectivity."

With regard to one final issue, in the NOPR, the Commission raised the need for security requirements related to the supply chain for hardware, software and computer services. FERC has decided to defer a decision on these issues until after a technical conference scheduled for January 28, 2016.

The changes ordered by FERC in Order No. 791, presented in the NOPR, and approved in Order No. 822 are as follows:

Eliminate "identify, assess and correct" language used in 17 of the CIP Version 5 Standard requirements

The Commission directed the removal of this language on the grounds that it was "overly vague, lacking basic definition and guidance that is needed, for example, to distinguish a successful internal control program from one that is inadequate."[2] The language was included in the original draft of the standards as a move away from a "zero-tolerance" enforcement approach, which was particularly onerous with regard to the cybersecurity standards. In ordering NERC to remove the language, FERC recognized, and approved of, the ultimate goal of moving away from a zero-tolerance model, but suggested that NERC propose modifications that would make the language of the provisions less ambiguous and easier to enforce.

NERC complied by removing the offending language and noted in its Petition[3] that its move away from a zero-tolerance approach is now reflected in its Compliance Monitoring and Enforcement Program due to changes made in NERC's enforcement procedures by the Reliability Assurance Initiative (RAI). The RAI is a broad initiative to move toward a risk-based approach to compliance monitoring and enforcement that started in 2012. NERC believes that changes made by the RAI will "directly accomplish" the goals of the "identify, assess and correct" language,[4] in particular, by using risk assessments and incenting utilities to develop internal controls to manage cybersecurity risks, with minor violations being addressed outside a formal enforcement action.

Provide enhanced security controls for Low Impact BES Cyber Assets

In the original version of the CIP Version 5 standards, there was only one standard applicable to Low Impact BES Cyber Assets, namely Reliability Standard CIP-003-5, Requirement R2, which required only very vague and general control measures to protect these assets. As a result, FERC ordered NERC to revise the standard to include specific objective criteria by which to judge the sufficiency of controls for protection of Low Impact BES Cyber Assets, which, FERC suggested, NERC could address by developing specific controls for Low Impact BES Cyber Assets.[5]

NERC opted to adopt specific security objectives for Low Impact BES Cyber Assets that require entities to develop and implement documented plans to "(1) regularly reinforce cybersecurity awareness and best practices across the organization; (2) establish protections to control physical access; (3) establish electronic access controls to limit inbound and outbound communication; and (4) implement Cyber Security Incident response plans."[6] However, NERC also opted to leave the specifics up to the responsible entity so that it would have the "flexibility to implement security controls for low impact BES Cyber Systems in the manner that best suits the needs and characteristics of their organization, so long as the responsible entity can demonstrate that it designed its controls to meet the ultimate security objectives."[7]

Provide controls to address the risks posed by transient electronic devices used at High and Medium Impact BES Cyber Assets

Transient electronic devices can be easily transported in and out of secure areas. Such devices are excluded from the standard definition of BES Cyber Asset, because it would be unduly burdensome to treat them in the same way as permanent cyber assets. However, FERC was concerned that such devices were not sufficiently protected under CIP Version 5, and it directed NERC to address the risks these devices might pose to the BES (such as the introduction of viruses or other malicious code).

NERC, in response, revised the CIP standards to require entities to develop plans and implement cybersecurity controls to protect transient devices associated with their High Impact and Medium Impact BES Cyber Assets. These controls include limiting who can use a given device, as well as limiting where, and for what reasons it may be used, and requiring that the software on such devices be kept up to date with security patches (or other methods of

addressing the risks of unpatched software). Entities are also required to train their personnel on the risks associated with using transient devices. The rules also address the risks posted by transient devices controlled by a third party, such as a vendor or contractor.

Create an NERC Glossary definition for the term "communication networks" and revise the standards for the protection of nonprogrammable components of communication networks

FERC was concerned that the CIP Version 5 standards did explicitly address security controls needed to protect the nonprogrammable components (such as cabling, wiring, hubs and ports) of communication networks and therefore directed NERC to adopt a definition of "communication networks" that would include these components. In addition, FERC directed NERC to adopt revised reliability standards that would provide for the protection of these components.

In this case, NERC concluded that it was not necessary to create such a definition, because the term "communication network" is not included in the CIP Version 5 standards. Further, NERC explained that it would be very hard to draft a definition that would be sufficiently broad while remaining accurate. Instead, "the standard drafting team simply identified the types of equipment or components that entities must protect and proposed appropriate and reasonable controls to secure those components based on the risks they present to the Bulk Electric System,"[8] noting that this approach will "meet the ultimate security objective of protecting communication networks (both programmable and nonprogrammable communication network components)."[9] NERC also revised several standards to address risks specifically concerning nonprogrammable components, requiring, for example, that certain cables be secured, either physically or digitally, to prevent "man-in-the-middle" type attacks. Another revision will require the elimination of unnecessary input/output ports.

---

[1] *Version 5 Critical Infrastructure Prot. Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

[2] Order No. 791 at P 4.

[3] NERC, Petition for Approval of Proposed Critical Infrastructure Protection Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2, Docket No. RM15-14-000 (filed Feb. 13, 2015) ("NERC Petition").

[4] NERC Petition at 5.

[5] Order No. 791 at PP 5, 106-08.

[6] NERC Petition at 25.

[7] *Id.*

[8] NERC Petition at 52.

[9] *Id.*

Categories

Energy Regulation, Markets & Enforcement