FERC Proposes Updates to Critical Infrastructure Protection Standards for Cybersecurity of Low Impact Bulk Electric System Operators

NOVEMBER 1, 2017

The Federal Energy Regulatory Commission (FERC) published a notice of proposed rulemaking (NPRM) on October 26, suggesting updates to the Critical Infrastructure Protection (CIP) Reliability Standard governing cybersecurity management controls for bulk electric system (BES) assets, called CIP-003.[1] The CIP program is a collection of standards designed to address the security of the bulk power system. Standards, and revisions thereto, are developed by the North American Electric Reliability Corporation (NERC) and are made mandatory and enforceable through acceptance and promulgation by FERC. CIP-003 governs "security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability."[2]

FERC Order 822

NERC developed the proposed revision, from the sixth version of CIP-003 to the proposed seventh version, in response to FERC Order 822. In that order, FERC directed NERC to revise CIP-003 (1) to clarify the obligations of operators of low impact BES Cyber Systems with respect to protecting against access from external users or devices and (2) to articulate standards for protecting against threats from transient devices, such as thumb drives.[3] NERC's revisions to CIP-003 address both directives, and FERC proposes to implement the standard as revised, while also proposing to direct NERC to make further refinements in each of these two areas.

Electronic Access Controls for Low Impact BES Cyber Systems

First, the proposed rule would revise section 3 of attachment 1 to CIP-003 to clarify the circumstances that trigger the obligation of responsible entities to establish electronic access controls for low impact BES Cyber Systems.[4] Under the existing standard, responsible entities must determine whether there exists Low Impact External Routable Connectivity (LERC), and if there is, implement a Low Impact BES Cyber System Electronic Access Point (LEAP). The definition of "LERC," however, is not a model of clarity, and FERC directed NERC to revise it in Order 822. NERC

took the matter a step further and threw out the terms LERC and LEAP altogether.

Under the proposed revision, responsible entities must implement protections that "[p]ermit only necessary inbound and outbound electronic access . . . between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s) [that use] a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s)."[5] FERC asserts that the proposal would rectify the confusion caused by the current definition of LERC and thus clarify when a responsible entity has an obligation. FERC, however, raises the concern that the new proposal "does not provide clear, objective criteria" by which to judge the adequacy of the control that a responsible entity must put in place, and directs NERC to modify the standard to provide such criteria, suggesting that the requirements for medium and high impact BES Cyber Systems could serve as a model.[6]

Transient Devices

Second, NERC's revision would add new sections to attachments 1 and 2 "to require responsible entities to include controls in their cyber security plans to mitigate the risk of the introduction of malicious code to low impact BES Cyber Systems" from transient devices.[7] The new sections provide that cyber security plans must include specific methods for detecting malicious code and mitigating the effects thereof. The new sections parallel the language in CIP-010-2, which sets standards for controlling similar risks to medium and high impact BES Cyber Systems, though the CIP-003 revisions exclude certain elements of CIP-010-2 relating to authorization and software vulnerabilities on the theory that industry resources should be focused on protecting the systems with greater potential to affect the bulk electric system.

FERC agrees that the revisions made "should improve the cybersecurity posture of responsible entities," but notes that the revisions fall short in one regard.[8] FERC identifies a continuing reliability gap in the fact that the standard, even as revised, does not oblige responsible entities to mitigate the introduction of malicious code from transient devices managed by third parties. FERC directs NERC to address this gap through further revisions to CIP-003.

Conclusion

Responsible entities that operate low impact BES Cyber Systems stand to be affected by the revisions to CIP-003, developed by NERC, and proposed by FERC to be put into force. They should also be aware of the further revisions to CIP-003 that NERC will undertake based on the directives issued by FERC in last week's NPRM. The proposal to accept the NERC revisions and the topics on which FERC suggests further modification are both subject to public comment until December 26.

---

[1] Federal Energy Regulatory Commission, "Revised Critical Infrastructure Protection Reliability Standard CIP-003-7—Cyber Security—Security Management Controls," 82 Fed. Reg. 49,541 (Oct. 26, 2017).

[2] CIP-003-7, "Cyber Security – Security Management Controls," § A.3.

[3] Federal Energy Regulatory Commission, "Revised Critical Infrastructure Protection Reliability Standards," Order No. 822, 154 FERC ¶ 61,037, at ¶ 3 (Jan. 21, 2016).

[4] "Responsible entity" is a term of art under CIP-003 encompassing the entities to which the standard generally applies and includes balancing authorities, distribution providers, generator owners and operators, interchange coordinators and authorities, reliability coordinators, and transmission owners and operators. CIP-003-7, at § A.4.1.

[5] CIP-003-7, Attach. 1, at § 3.1.

[6] 82 Fed. Reg. at 49,545.

[7] *Id*. at 49,545-46; *see* CIP-003-7, Attach. 1, § 5; Attach. 2, § 5.

[8] 82 Fed. Reg. at 49,546.