Akin®

FERC Directs NERC to Tighten Bulk Electric System Cybersecurity

January 26, 2023

Reading Time : **5 min**

By: Stephen J. Hug, Emily P. Mallen, Scott Daniel Johnson, Angelica Gonzalez (Paralegal)

These Reliability Standards will apply to *all* high impact BES Cyber Systems *with and without* external routable connectivity—*i.e.*, a high-speed internet connection[6]—and medium impact BES Cyber Systems *with* external routable connectivity.[7] FERC also directed NERC "to study the feasibility of implementing INSM at bulk electric cyber systems that would not be addressed by the new or modified standard[s]," [8] which include low impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems without external routable connectivity.[9]

The Final Rule will become effective 60 days after publication in the Federal Register.[10] NERC has 15 months to submit the new standards and 12 months to submit its study on low- and medium-impact systems.[11]

New Acting Chairman Willie L. Phillips commented that "[t]he nature of cyber security threats to our nation's grid require constant monitoring and vigilance," and FERC's action represents "a major step to better secure the reliability of our nation's bulk power system."[12] In a prior role, Chairman Phillips served as an Assistant General Counsel with NERC.

Overview

Under the current NERC CIP Reliability Standards, network security monitoring requirements focus on defending the electronic security perimeter—such as through access point controls and monitoring for malicious communications—rather than on potential vulnerabilities of the internal network.[13] Adding INSM requirements is "designed to address as early as possible

situations where perimeter network defenses are breached by detecting intrusions and malicious activity within a trust zone."[14] It consists of: (1) collection; (2) detection; and (3) analysis.[15] These three stages together "provide the benefit of early detection and alerting of intrusions and malicious activity."[16] Early detection and response can, in turn, "reduce[] the likelihood that an attacker can gain a strong foothold, including operational control, on the target system."[17] INSM can also enable "collection of data and analysis required to implement a defense strategy, improves an entity's incident investigation capabilities, and increases the likelihood that an entity can better protect itself from a future cyberattack and address any security gaps the attacker was able to exploit."[18]

While "NERC has flexibility in developing the content of INSM requirements, the new or modified CIP Reliability Standards must address [certain] specific concerns" FERC raised.[19] They must be "forward-looking, objective-based, and . . . address . . . three security objectives that pertain to INSM."[20] First, they "should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment."[21] Second, they "should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment."[22] Finally, they "should require responsible entities to identify anomalous activity to a high level of confidence by: (1) logging network traffic" (such as by packet capture); "(2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices."[23]

As to other BES Cyber Systems not covered by the new or revised Reliability Standards, FERC found that it is "premature" to require INSM for such systems, but also recognized "the importance of bolstering the cybersecurity of those systems," noting that "extending INSM to [such] BES Cyber Systems . . . in the future could be necessary to protect the security and the reliability of the Bulk-Power System."[24]

NERC Study Regarding Lower-Impact Systems

In NERC's study of such BES Cyber Systems, FERC directed that NERC "should include . . . a determination of: (1) ongoing risk to the reliability and security of the Bulk-Power System posed by low and medium impact BES Cyber Systems that would not be subject to the new

or modified Reliability Standards, including the number of low and medium impact BES Cyber Systems not required to comply with the new or modified standard; and (2) potential technological or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative mitigating actions to address ongoing risks."[25] FERC may use this information to provide a basis "for further Commission action, as warranted, regarding INSM or alternatives."[26] NERC's study is due within a year of the effective date of the Final Rule.[27]

Recommendations

Entities that own or operate high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity should, at a minimum, continue to monitor NERC's Reliability Standards development process and consider participating in that process and/or the FERC proceeding in which NERC submits its proposed standards. Those entities with medium impact BES Cyber Systems without external routable connectivity or low impact BES Cyber Systems should review NERC's study report for indications about what more, if anything, NERC or FERC might do going forward with respect to such systems. This remains a rapidly evolving area with the potential to create additional cybersecurity risk, compliance costs and liability for affected entities. Stay ahead by staying informed.

---

[1] *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Order No. 887, 182 FERC ¶ 61,021 (2023) ("Final Rule"). *See also* FERC, News Release, FERC Strengthens Reliability Standards for Monitoring Electric Grid Cyber Systems (Jan. 19, 2023) ("FERC News Release") (available here).

[2] Final Rule at P 20. *See also id.* at PP 39, 50.

[3] *Id.* at P 3. *See also id.* at PP 19, 80.

[4] *Id.* at PP 15, 50.

[5] *Id.* at P 15. *See also id.* at PP 3, 50.

[6] "External routable connectivity" is the "ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." *Id.* n.3 (quoting NERC, Glossary of Terms Used in NERC Reliability Standards (2022) (NERC Glossary), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf).

[7] *Id.* at P 1. NERC's CIP Reliability Standards categorize BES Cyber Systems "as high, medium, or low impact depending on the functions of the assets housed within each system and the risk they potentially pose to the reliable operation of the Bulk-Power System." *Id.* n.2. The designated impact level then "determines the applicability of security controls for BES Cyber Systems that are contained in the remaining CIP Reliability Standards (i.e., Reliability Standards CIP-003-8 to CIP-013-1)" as they currently exist. *Id.* In early 2022, FERC had proposed to direct NERC to address INSM for all high and medium impact BES Cyber Systems, but limited the requirement in the Final Rule in response to stakeholder comments. *Id.* at P 4 (citing *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Notice of Proposed Rulemaking, 178 FERC ¶ 61,038 (2022)).

[8] *E.g.*, FERC News Release at 1.

[9] Final Rule at PP 1, 88.

[10] *Id.* at P 104.

[11] *E.g.*, *id.*, at PP 1, 6.

[12] FERC News Release at 1.

[13] *See, e.g.*, Final Rule at PP 3, 14.

[14] *Id.* at P 9.

[15] *Id.*

[16] *Id.*

[17] *Id.* at P 13.

[18] *Id.* at P 49.

[19] *Id.* at P 5.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* (footnotes omitted). *See also id.* at P 77.

[24] *Id.* at P 88.

[25] *Id.* at P 7. *See also id.* at P 88.

[26] *Id.* at P 7. *See also id.* at PP 31, 88.

[27] *E.g.*, *id.* at P 91.

Categories

Cybersecurity & Information Security | Energy & Infrastructure

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.