178 FERC ¶ 61,038
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM22-3-000]

Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems

(Issued January 20, 2022)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to direct the North American Electric Reliability Corporation to develop and submit for Commission approval new or modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for high and medium impact Bulk Electric System Cyber Systems.

DATES: Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways. Electronic filing through https://www.ferc.gov, is preferred.

- Electronic Filing: Documents must be filed in acceptable native applications and print-to-PDF, but not in scanned or picture format.
- For those unable to file electronically, comments may be filed by U.S. Postal Service mail or by hand (including courier) delivery.

- Mail via U.S. Postal Service only: Addressed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street NE, Washington, DC 20426.
- For delivery via any other carrier (including courier): Deliver to: Federal Energy Regulatory Commission, Office of the Secretary, 12225 Wilkins Avenue, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT:

Cesar Tapia (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6559
cesar.tapia@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

Milena Yordanova (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6194
milena.yordanova@ferc.gov

SUPPLEMENTARY INFORMATION:

178 FERC ¶ 61,038
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Richard Glick, Chairman;
James P. Danly, Allison Clements,
Mark C. Christie, and Willie L. Phillips.

Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems — Docket No. RM22-3-000

NOTICE OF PROPOSED RULEMAKING

(Issued January 20, 2022)

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission proposes to direct the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), to develop new or modified Reliability Standards that require network security monitoring internal to a Critical Infrastructure Protection (CIP) networked environment (internal network security monitoring or INSM) for high and medium impact Bulk Electric System (BES) Cyber Systems.[2] INSM is a subset of network security monitoring that is applied within a "trust

[1] 16 U.S.C. 824o(d)(5).

[2] Reliability Standard CIP-002-5.1a (BES Cyber System Categorization) sets forth criteria that registered entities apply to categorize BES Cyber Systems as high, medium, or low depending on the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. The impact level (i.e., high, medium, or low) of BES Cyber Systems, in turn, 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).

zone,"[3] such as an Electronic Security Perimeter (ESP),[4] and is designed to address situations where vendors or individuals with authorized access are considered secure and trustworthy but could still introduce a cybersecurity risk to a high or medium impact BES Cyber System.

2. Although the currently effective CIP Reliability Standards offer a broad set of cybersecurity protections, they do not address INSM. This omission constitutes a gap in the CIP Reliability Standards. Including INSM requirements in the CIP Reliability Standards would ensure that responsible entities maintain visibility over communications between networked devices within a trust zone (i.e., within an ESP), not simply monitor communications at the network perimeter access point(s), i.e., at the boundary of an ESP as required by the current CIP requirements. In the event of a compromised ESP, improving visibility within a network would increase the probability of early detection of malicious activities and would allow for quicker mitigation and recovery from an attack.

---

[3] A trust zone is defined as a "discrete computing environment designated for information processing, storage, and/or transmission that share the rigor or robustness of the applicable security capabilities necessary to protect the traffic transiting in and out of a zone and/or the information within the zone." U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), *Trusted Internet Connections 3.0: Reference Architecture*, at 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf.

[4] The NERC Glossary defines an ESP as "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." NERC, *Glossary of Terms Used in NERC Reliability Standards* (June 28, 2021), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

In addition to improved incident response capabilities and situational awareness, INSM also contributes to better vulnerability assessments within an ESP, all of which support an entity's cybersecurity defenses and could reduce the impact of cyberattacks.

3. While the currently effective CIP Reliability Standards do not require INSM, NERC has recognized the proliferation and usefulness of network monitoring technology on the BES. For example, on January 4, 2021, NERC issued a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide addressing Network Monitoring Sensors, Centralized Collectors, and Information Sharing.[5] NERC explained that the CMEP Practice Guide was developed in response to a U.S. Department of Energy (DOE) initiative "to advance technologies and systems that will provide cyber visibility, detection, and response capabilities for [industrial control systems] of electric utilities."[6] As discussed below, in view of these and other ongoing efforts to improve network monitoring, we believe that there is a sufficient basis for a directive to NERC to require INSM in the CIP Reliability Standards for high and medium impact BES Cyber Systems.

4. We seek comments on all aspects of the proposed directive to NERC to modify the CIP Reliability Standards to require INSM for high and medium impact BES Cyber Systems. The proposed directive centers on high and medium impact BES Cyber Systems in order to improve visibility within networks containing BES Cyber Systems

---

[5] NERC, *ERO Enterprise CMEP Practice Guide: Network Monitoring Sensors, Centralized Collectors*, *and Information Sharing* (June 4, 2021), https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf (CMEP Practice Guide).

[6] *Id.* at 1.

whose compromise could have a significant impact on the reliable operation of the BES. However, because low impact BES Cyber Systems have fewer security controls than high and medium impact BES Cyber Systems, we also seek comments on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low impact BES Cyber Systems, including any potential benefits, technical barriers and associated costs.

5. Upon review of the filed comments, the Commission will consider whether to broaden the directives in the final rule to direct NERC to require INSM in the CIP Reliability Standards for low impact BES Cyber Systems or a defined subset of low impact BES Cyber Systems.

I. Background

A. Section 215 and Mandatory Reliability Standards

6. Section 215 of the FPA requires the Commission to certify an ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[7] Once approved, the Reliability Standards are enforceable in the United States by the ERO, subject to Commission oversight, or by the Commission independently.

[7] 16 U.S.C. 824o.

Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[8] and subsequently certified NERC.[9]

B. Network Security Monitoring and Internal Network Security Monitoring

1. Network Security Monitoring in Currently Effective CIP Reliability Standards

7. Currently, network security monitoring in the CIP Reliability Standards focuses on network perimeter defense and preventing unauthorized access at the network perimeter. While responsible entities are required to have a security program to implement various controls,[10] Reliability Standard CIP-005-6 (Electronic Security Perimeter(s)), Requirement R1.5 is the only requirement that addresses monitoring of network traffic for malicious communications at the ESP. In particular, this provision requires a responsible entity to have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. Under

---

[8] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards,* Order No. 672, 71 FR 8662 (Feb. 17, 2006), 114 FERC ¶ 61,104, *order on reh'g,* Order No. 672-A, 71 FR 19814 (Apr. 18, 2006), 114 FERC ¶ 61,328 (2006).

[9] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[10] *See*, *e.g.*, (1) network perimeter defenses (CIP-005-7, Requirement R1 – Electronic Security Perimeter); (2) sensitive information control (CIP-011-2 – Information Protection, CIP-004-6, Requirement R4 – Access Management Program, and CIP-004-6, Requirement R5 – Access Revocation); (3) anti-malware (CIP-007-6, Requirement R3 – Malicious Code Prevention); (4) security awareness and training (CIP-004-6, Requirement R1 – Security Awareness Program and CIP-004-6, Requirement R2 – Cyber Security Training Program); and (5) configuration change management (CIP-010-4, Requirement R1 – Configuration Change Management).

Requirement R1.5, the only locations that require network security monitoring are the ESP electronic access points for high and medium impact BES Cyber Systems at control centers. The currently effective CIP Reliability Standards do not require entities to have a defined ESP for low impact BES Cyber Systems and, therefore, there is no requirement for network security monitoring for inbound or outbound communication of such systems.

8. The CIP Reliability Standards also require entities to install security monitoring tools at the device level. For instance, Reliability Standard CIP-007-6 (System Security Management), Requirement R.4.1.3 addresses security monitoring and requires the entity to detect malicious code for all high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets. To comply with Reliability Standard CIP-007-6 (Systems Security Management), Requirement R.4.1.3, a responsible entity is not required to use INSM methods, such as an intrusion detection system.[11]

2. Internal Network Security Monitoring

[11] Under Reliability Standard CIP-007-6, Requirement R.4.1.3, an entity may choose, but is not required, to use system generated listing of network log in/log outs, or malicious code, or other types of monitored network traffic at the perimeter of all high and medium impact BES Cyber Systems. *See* Reliability Standard CIP-007-6 (Cyber Security – Systems Security Management), Requirement R.4.1.3, Measures (stating that examples of evidence of compliance may include, but are not limited to, a paper or system generated listing of monitored activities for which the BES Cyber System is configured to log and capable of detecting).

9. INSM refers to network security monitoring inside of a trust-zone. INSM is designed to address situations where perimeter network defenses are breached by providing the earliest possible alerting and detection of intrusions and malicious activity within a trust zone. INSM consists of three stages: (1) collection; (2) detection; and (3) analysis that, taken together, provide the benefit of early detection and alerting of intrusions and malicious activity.[12] Some of the tools used for INSM include: anti-malware; Intrusion Detection Systems; Intrusion Prevention Systems; and firewalls.[13] These tools are multipurpose and can be used for collection, detection, and analysis (e.g., forensics). Additionally, some of the tools (e.g., anti-malware, firewall, or Intrusion Prevention Systems) have the capability to block network traffic.

10. The benefits of INSM can be understood by first describing the way attackers commonly compromise targets. Attackers typically follow a systematic process of planning and execution to increase the likelihood of a successful compromise.[14] This

---

[12] *See* Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013).

[13] *See* NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, at pp. 10-13 (July 2013) (Explaining that anti-malware tools find and remove malware. Intrusion Detection Systems monitor a network for anomalous activity, which includes malicious activity or policy violations, and report them to security teams for further analysis. A firewall monitors and controls incoming and outgoing network traffic).

[14] A widely accepted cybersecurity attack framework for describing the process that an effective adversary typically follows to increase the probability of a successful compromise is referred to as Cyber Kill Chain. The Cyber Kill Chain provides more detail on the specific steps that an attacker could follow. SANS Institute, *Applying*

process includes: reconnaissance (e.g., information gathering); choice of attack type and method of delivery (e.g., malware delivered through a phishing campaign); taking control of the entity's systems; and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information).[15] Successful cyberattacks require the attacker to gain access to a target system and execute commands while in that system.

11. INSM could better position an entity to detect malicious activity that has circumvented perimeter controls. Because an attacker that moves among devices internal to a trust zone must use network pathways and required protocols to send malicious communications, INSM will potentially alert an entity of the attack and improve the entity's ability to stop the attack at its early phases.

12. By providing visibility of network traffic that may only traverse internally within a trust zone, INSM can warn entities of an attack in progress. For example, properly placed, configured, and tuned INSM capabilities such as intrusion detection system and intrusion prevention system sensors could detect and/or block malicious activity early and alert an entity of the compromise. INSM can also be used to record network traffic for analysis, providing a baseline that an entity can use to better detect malicious activity. Establishing baseline network traffic allows entities to define what is and is not normal

---

Security Awareness to the Cyber Kill Chain, (May 2019), https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/.

[15] *Id.*

and expected network activity and determine whether observed anomalous activity warrants further investigation.[16] The collected network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious activity.

13. In summary, INSM better postures an entity to detect an attacker in the early phases of an attack and reduces the likelihood that an attacker can gain a strong foothold and potential command and control, including operational control, on the target system. In addition to early detection and mitigation, INSM may improve incident response by providing higher quality data about the extent of an attack internal to a trust zone. High quality data from collected network traffic is important for recovering from cyberattacks as this type of data allows for: (1) determining the timeframe for backup restoration; (2) creating a record of the attack for incident response and reporting; and (3) analyzing the attack itself to prevent it from happening again (e.g., through lessons learned that can improve organizational policies, processes, and playbooks).[17] Finally, INSM allows entities to conduct internal assessments and prioritize any improvements based on their risk profile.[18]

---

[16] *See* CISA, *Best Practices for Securing Election Systems*, Security Tip (ST19-002), (Aug. 2021), https://www.cisa.gov/tips/st19-002.

[17] Help Net Security, *Three Reasons Why Ransomware Recovery Requires Packet Data*, (Aug. 2021), https://www.helpnetsecurity.com/2021/08/24/ransomware-recovery-packet-data/.

[18] CISA, *CISA Analysis: FY2020 Risk and Vulnerability Assessments*, (July 2021), https://www.cisa.gov/sites/default/files/publications/FY20-RVA-Analysis_508C.pdf.

II. Discussion

14. As discussed below, we believe that the absence of a requirement to conduct INSM for CIP networked environments containing high and medium impact BES Cyber Systems constitutes a gap in the Reliability Standards. Accordingly, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop new or modified Reliability Standards that address the use of INSM for high and medium impact BES Cyber Systems. We believe that requiring entities to implement INSM will improve visibility and awareness of communications between networked devices and between devices internal to trust zones (i.e., ESPs), and increase the probability of detecting and mitigating malicious activity in the early phases of an attack.

15. We also seek comments on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low impact BES Cyber System, including any potential benefits, technical barriers, and associated costs. The Commission may broaden its directive in a final rule to include low impact BES Cyber Systems, or some subset of low impact BES Cyber Systems, if the filed comments support such a directive. While the high and medium impact categories have defined thresholds, the low impact category of BES Cyber Systems is essentially a broad group of all BES Cyber Systems that do not satisfy the high or medium impact thresholds. Identifying a subset of low impact BES Cyber Systems to which INSM provisions would apply could allow entities to focus their resources on the assets with a more significant risk profile within the broad low impact tier of BES Cyber Systems. For example, a subset of low impact BES Cyber Systems to which INSM provisions could apply may be contained within control centers

and backup control centers, transmission stations and substations, and/or generation resources.[19]

16. In the following sections, we discuss: (A) current risks to trusted CIP networked environments; (B) how INSM is a widely recognized control against cyberattacks; (C) how the absence of INSM constitutes a gap in the CIP Reliability Standards; and (D) how the proposed directive would address the gap.

A. Risks to Trusted CIP Networked Environment

17. Currently, the NERC CIP Reliability Standards require monitoring of the ESP and associated systems for high and medium impact BES Cyber Systems. However, even when the ESP is monitored and protected, the CIP networked environment (i.e., trust zone) remains vulnerable to cyber threats like insider threats or supply chain attacks initiated by an adversary by infiltrating a trusted vendor, among other attack vectors. In the context of supply chain risk, a malicious update from a known software vendor could be downloaded directly to a server as trusted code, and it would not set-off any alarms until abnormal behavior occurred and was detected. Because the CIP networked environment is a trust zone, the compromised server in the trust zone could be used to install malicious updates directly onto devices that are internal to the CIP networked environment without detection. In the context of an insider threat, an employee with

[19] Reliability Standard CIP-002-5.1a (Cyber Security — BES Cyber System Categorization), Attachment 1, Section 3 (explaining that low impact rating is assigned to BES Cyber Systems that, among other requirements, are associated with assets such as control centers and backup control centers, transmission stations and substations, generation resources, etc.).

elevated administrative credentials could identify and collect data, add additional accounts, delete logs, or even exfiltrate data without being detected.

18. For example, the recent SolarWinds attack demonstrates how an attacker can bypass all network perimeter-based security controls traditionally used to identify the early phases of an attack.[20] On December 13, 2020, FireEye Inc., a cybersecurity solutions and forensics firm, identified a global intrusion campaign that introduced a compromise delivered through updates to the Orion network monitoring product from SolarWinds, a widely used IT infrastructure management software.[21] This supply chain attack leveraged a trusted vendor to compromise the networks of public and private organizations, and it was attributed by the U.S. government to the Russian foreign intelligence service.[22] SolarWinds customers had no reason to suspect the installation of compromised updates because the attacker used an authenticated SolarWinds certificate. This attack bypassed all network perimeter-based security controls traditionally used to identify the early phases of an attack.

---

[20] *See* FERC, NERC, *SolarWinds and Related Supply Chain Compromise,* at 16 (July 7, 2021), https://cms.ferc.gov/media/solarwinds-and-related-supply-chain-compromise-0.

[21] FireEye, *Global Intrusion Campaign Leverages Software Supply Chain Compromise*, (2020), https://www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html.

[22] The White House, *Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government*, (April 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

19. The supply chain is not the only attack vector used to gain malicious access to a system. While not jurisdictional for purposes of our reliability standards, the May 2021 large-scale ransomware attack targeting Colonial Pipeline provides an important example of an attack via one such vector that could halt an entity's operations.[23] In this case, the attacker gained the credentials to and exploited a legacy virtual private network profile that was not intended to be in use.[24] Although this attack was directed at the information technology (IT) systems of the pipeline, Colonial Pipeline decided to shut down operations as a precaution.[25] With tools such as INSM, a shutdown of operations may not be necessary as entities are better postured to timely detect and mitigate similar

[23] Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption* (May 9, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption (stating that after learning of the attack, Colonial took certain systems offline to contain the threat. These actions temporarily halted all pipeline operations and affected some of Colonial's IT systems) (May 9, 2021 Colonial Pipeline Media Statement Update); Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption*, (May 8, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption (On May 7, 2021 Colonial Pipeline Company learned it was the victim of a cybersecurity attack and determined that the incident involved ransomware).

[24] Hearing Before The United States House Of Representatives Committee On Homeland Security (117th Congress), Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company, at 4 (June 9, 2021), https://www.congress.gov/117/meeting/house/112689/witnesses/HHRG-117-HM00-Wstate-BlountJ-20210609.pdf. *See also* Reuters, *One Password Allowed Hackers to Disrupt Colonial Pipeline*, CEO Tells Senators (June 8, 2021), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/ (explaining that the legacy virtual private network had single-factor authentication, a password, and did not have a multi-factor authentication requirement in place).

[25] May 9, 2021 Colonial Pipeline Media Statement Update.

events in which an adversary successfully penetrates perimeter defenses and moves freely within the internal network.

20. In addition to early detection, INSM is critical for identifying malicious activities at the later stages of cybersecurity attacks. Absent INSM, an entity may not be alerted if an adversary establishes a command and control communication channel that interacts with the compromised system on a regular basis.[26] Once an attacker proceeds to the last phase of an attack, the attacker will have had time to compromise multiple devices, steal user credentials, and map the network extensively.[27] Removing an attacker at this level of penetration can be time consuming (e.g., months to years), costly, and extremely difficult.

21. The serious operational consequences of such undetected penetration into a networked environment for the BES could include: (1) loss of situational awareness monitoring; (2) loss of coordination capabilities during reliability events and system restoration activities; (3) unexpectedly large power flows; (4) loss of voice or data communication; (5) loss of protection systems; (6) loss of electric generation,

---

[26] A command and control communication channel is used to issue instructions to the compromised devices, download additional malicious payloads (e.g. malware), which sit harmlessly until triggered, and exfiltrate data. *See* NSA, *Cybersecurity Report: NSA/CSS Technical Cyber Threat Framework* (Nov. 2018), https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/ctr-nsa-css-technical-cyber-threat-framework.pdf.

[27] Network mapping is used to compile an electronic inventory of the systems and the services on the network. *See* SANS Institute, *Glossary of Terms*, https://www.sans.org/security-resources/glossary-of-terms.

transmission, or fuel supply, water supply/coolant; (7) power market disruption; and (8) loss of Critical Energy/Electric Infrastructure Information.[28] For example, if an attacker compromises high and/or medium impact BES Cyber Systems internal to a CIP networked environment (i.e., trust zone) without INSM, the attacker could communicate with and move freely between devices within a trust zone with little likelihood of detection. The attacker could then access the Supervisory Control and Data Acquisition (SCADA)[29] system and control equipment like circuit breakers[30] dropping generating resources or load, and potentially causing BES instability or uncontrolled separation.[31]

B. INSM is a Widely Recognized Control Against Cyberattacks

22. Elements of INSM have been recognized and recommended by government officials and industry experts as necessary for the early detection and mitigation of

---

[28] SERC Reliability Corporation, *2020 SERC Reliability Risk Report*, (Sept. 21, 2020), https://www.serc1.org/docs/default-source/committee/ec-reliability-risk-working-group/2020-reliability-risk-report.pdf?sfvrsn=e80ea39_2.

[29] SCADA is a system that aims to monitor and control field devices at remote sites. SCADA systems are critical as they help maintain efficiency by collecting and processing real-time data. *See* DPS Telecom, *How Do SCADA Systems Work?*, https://www.dpstele.com/scada/how-systems-work.php.

[30] A circuit breaker is an electrical switch designed to protect an electrical circuit from damage caused by overcurrent/overload or short circuit. Its basic function is to interrupt current flow after protective relays detect a fault. *See* Eaton, *Circuit Breaker Fundamentals*, https://www.eaton.com/us/en-us/products/electrical-circuit-protection/circuit-breakers/circuit-breakers-fundamentals.html.

[31] Electricity Information Sharing and Analysis Center (E-ISAC), *Modular ICS Malware* (Aug. 2017), https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICS_Malware%20Final.pdf?parent=64412.

cyberattacks. For example, on May 12, 2021, the President issued Executive Order No. 14,028 on Improving the Nation's Cybersecurity,[32] which directly addresses cyber protection through increased visibility and data collection.[33] The Executive Order directs the federal government and encourages the private sector to implement several aspects of INSM and emphasizes that the federal government must improve its efforts to identify, deter, protect against, detect, and respond to the actions of sophisticated malicious actor cyber campaigns that threaten the security and privacy of the public sector, private sector, and the American people.[34] Further, the Executive Order instructs federal agencies, among other things, to modernize their approach to cybersecurity by increasing visibility into threats and advancing toward zero trust principles;[35] allocating resources to

[32] Executive Order No. 14,028, 86 FR 26633 (May 12, 2021), https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[33] The scope of protection includes systems that process data (i.e., information technology) and those that run the vital machinery that ensures safety (i.e., operational technology).

[34] Executive Order No. 14,028, 86 FR 26633, 26635, 26643 (May 12, 2021) (mandating that the "Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks" and "increas[e] the Federal Government's visibility into threats." The Executive Order further emphasizes that "cybersecurity requires more than government action" and "[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.").

[35] *Id*. at 26635. Executive Order No. 14,028 refers to zero trust architecture. Zero trust is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the

maximize early detection of cybersecurity vulnerabilities and incidents on networks;[36] and collecting and maintaining information from network and system logs, as they are invaluable tools for investigation and remediation.[37]

23. In addition, on July 28, 2021, the President signed the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (National Security Memorandum) to comprehensively address cybersecurity for critical infrastructure.[38] The President emphasizes that "[r]ecent high-profile attacks on critical infrastructure around the world, including the ransomware attacks on the Colonial Pipeline and JBS Foods in the United States, demonstrate that significant cyber vulnerabilities exist across U.S. critical infrastructure, which is largely owned and

---

internet) or based on asset ownership (enterprise or personally owned). *See generally* National Institute of Standards and Technology (NIST), *NIST Special Publication 800-207 Zero Trust Architecture*, (Aug. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (providing a general definition of zero trust and general information and cases where zero trust may improve an entity's overall cybersecurity posture).

[36] Executive Order No. 14,028, 86 FR 26633, 26643 (May 12, 2021).

[37] *Id*. at 26644.

[38] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, Section 2 (Industrial Control Systems Cybersecurity Initiative), (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ (National Security Memorandum). *See also* The White House, *Fact Sheet: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure*, (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/) (The White House July 28, 2021 Fact Sheet).

operated by the private sector."[39] The National Security Memorandum established an Industrial Control Systems Cybersecurity Initiative (Cybersecurity Initiative) to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings.[40] The Cybersecurity Initiative started with a pilot in the electricity sector and has wide participation, including participation by vendors that have implemented INSM in their products.[41]

24. Furthermore, CISA and NIST have recommended detailed cybersecurity practices, which include elements of INSM, such as recommending that organizations conduct network baseline analysis on control systems and networks to understand approved communication flows and to monitor control systems for malicious activity on control systems.[42] Similarly, CISA and the Federal Bureau of Investigation published a joint cybersecurity advisory in response to illicit activities by a Chinese group known as

[39] The White House July 28, 2021 Fact Sheet. JBS is a meat processing company, which shut down all of its beef processing plants in the USA as a result of a ransomware attack. *See* U.S. Department of Agriculture, *Statement from the U.S. Department of Agriculture on JBS USA Ransomware Attack*, (June 2021), https://www.usda.gov/media/press-releases/2021/06/01/statement-us-department-agriculture-jbs-usa-ransomware-attack.

[40] National Security Memorandum, Section 2 (Industrial Control Systems Cybersecurity Initiative).

[41] White House July 28, 2021 Fact Sheet.

[42] CISA, *Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives* (Sept. 21, 2021), https://www.cisa.gov/control-systems-goals-and-objectives.

APT40.[43] The activities of APT40 resulted in the theft of trade secrets, intellectual property, and other high-value information from companies and organizations in the United States and abroad.[44] The joint cybersecurity advisory recommended deployment of INSM measures such as active scanning and monitoring of internet-accessible applications for unauthorized access, modification, and anomalous activities; logging domain name service queries; developing and monitoring network and system baselines to allow for the identification of anomalous activity; and using baseline comparison to monitor Windows event logs and network traffic to detect when a user maps a privileged administrative share on a Windows system.[45]

25. Industry and government cybersecurity experts also supported the use of INSM at the Commission's 2021 Annual Reliability Technical Conference.[46] Panelists discussed the importance of improved visibility to detect cyberattacks by implementing network

[43] Joint Cybersecurity Advisory, *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*, (July 19, 2021), https://www.cisa.gov/uscert/sites/default/files/publications/CSA_TTPs-of-Indicted-APT40-Actors-Associated-with-China-MSS-Hainan-State-Security-Department.pdf.

[44] *Id*. at 1.

[45] *Id*. at 4-5.

[46] Federal Energy Regulatory Commission, *2021 Annual Reliability Technical Conference,* Transcript, Panel 3: Managing Cyber Risks in the Electric Power Sector, Docket No. AD21-11-000 (Sept. 30, 2021), https://www.ferc.gov/news-events/events/annual-commissioner-led-reliability-technical-conference-09302021.

capabilities like INSM.[47] One panelist observed that recent attacks like SolarWinds and Colonial Pipeline "demonstrated how a coordinated attack could compromise our systems," and that they "really underscore[] the need for heightened visibility... more comprehensive logging of events, potentially other controls that you know go across all asset environments, but it should be done in a risk based way."[48] Another panelist discussed additional benefits of INSM, stating that monitoring and having the appropriate logs are essential to perform a root cause analysis and understand the sequence of events that occurred, and collection of data (i.e., logs), enabled by INSM, is also essential to gaining a deeper understanding of a cyberattack.[49]

C. The Absence of INSM Constitutes a Gap in the Reliability Standards

26. While NERC's approved CIP Reliability Standards provide a broad set of cybersecurity protections, they do not require INSM. Currently, the only locations that require network security monitoring are the electronic access points at high and medium impact BES Cyber Systems at control centers. In these zones, trusted vendors or authorized individuals are the only users with access, but they are not subject to monitoring under the CIP Reliability Standards. Implementing INSM will help to detect and mitigate situations where malicious actors exploit this gap.

---

[47] *Id*. at 165 (Ben Miller, Vice President, Services and R&D, Dragos Inc.); 178:14:23 (Mark Fabro, President and Chief Security Scientist, Lofty Perch).

[48] *Id*. at 200 (Manny Cancel, Senior Vice President and Chief Executive Officer, NERC E-ISAC).

[49] *Id*. at 202:8-19 (Miller).

27. Given the increased sophistication of cyberattacks, relying on network perimeter defense and other existing controls leaves trust zones vulnerable. As the President's Deputy National Security Advisor for Cyber and Emerging Technology explained "[i]f you can't see a network, you can't defend a network."[50] Panelists at the Commission's 2021 Annual Reliability Technical Conference confirmed this gap in the CIP Reliability Standards, explaining that there is "implementation of perimeter controls and some other protective controls, and some planning, but there is not a concept around detection and monitoring."[51] An estimate from a security vendor panelist indicates that 70% of the NERC CIP Reliability Standards are focused on prevention, and the remaining 30% focus on other protection measures, including monitoring.[52] Panelists supported the view that monitoring within a trust zone is critical, underscoring the need to close the reliability gap in the currently effective Reliability Standards.[53] This is particularly important as the

[50] The White House, *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger*, (Feb. 17, 2021), https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/.

[51] 2021 Annual Reliability Technical Conference, Tr. 201:20-25; 202:1-7 (Miller).

[52] *Id*.

[53] *Id*. at 202:22-23 (Tony Hall, Manager, CIP Program, Louisville Gas and Electric Company and Kentucky Utilities Company).

energy sector undergoes a digital transformation, which creates new cyber threat pathways.[54]

28. NERC facilitated the voluntary use of INSM in its CMEP Practice Guide, which provides guidance on how to incorporate network sensors in the ESP while being compliant with the CIP Reliability Standards. These network sensors enable entities to use INSM, if they choose, and support implementation of the Essence Cybersecurity Tool.[55] However, the CMEP Practice Guide does not modify the CIP Reliability Standards to require INSM, leaving unaddressed the cybersecurity gap within trust zones.

D. The Commission Proposed Directive Addresses the Identified Reliability Gap

29. Pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop new or modified CIP Reliability Standards that require security controls for INSM for high and medium impact BES Cyber Systems. Based on the current threat environment discussed above, a requirement for INSM that augments existing perimeter defenses is critical to increasing network visibility so that an entity may understand what is occurring in its CIP networked environment, and thus improve capability to timely detect potential

[54] *Id*. at 170:24-25; 171:1 (Puesh Kumar, Acting Principal Deputy Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy).

[55] National Rural Electric Cooperative Association (NRECA), *DOE Awards NRECA $6M to Take Essence Cybersecurity Tool to the Next Level* (Sept. 29, 2020), https://www.electric.coop/doe-gives-nreca-6m-to-take-essence-cybersecurity-tool-to-the-next-level; NRECA, *New Cyber Technology Provides Real-Time Defense* (March 15, 2021), https://www.electric.coop/new-essence-cyber-technology-provides-real-time-defense.

compromises. INSM also allows for the 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.

30. The proposal to direct NERC to add an INSM requirement to the existing set of CIP Reliability Standard is also consistent with Executive Order No. 14,028, which calls for employing a zero trust cybersecurity approach, and the objectives of the President's July 2021 Cybersecurity Initiative targeting deployment of control system cybersecurity technologies in the electricity and other critical sectors. INSM is a fundamental element of the zero trust approach and should improve the cybersecurity posture of responsible entities with high and medium impact BES Cyber Systems.

1. High and Medium Impact BES Cyber Systems

31. To address the reliability gap and improve cybersecurity, we propose to direct that NERC, as the ERO, develop new or modified CIP Reliability Standards requiring that applicable responsible entities implement INSM for their high and medium impact BES Cyber Systems. Such new or modified Reliability Standards should address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for each responsible entity to develop a baseline for their network traffic by analyzing expected network traffic and data flows for security purposes. This objective reduces the likelihood that an attacker could exploit legitimate cyber resources to: (1) escalate privileges, i.e., exploit software vulnerability to gain administrator account privileges; (2) move undetected inside a CIP networked

environment (i.e., trust zone); and (3) execute unauthorized code, e.g., a virus or ransomware. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP networked environment (i.e., trust zone). This objective reduces detection time, which shortens the time an attacker has to leverage compromised user accounts and traverse over unmonitored network connections. And third, any new or modified CIP Reliability Standards should address the ability to support operations and response by requiring responsible entities to: (1) log and packet capture[56] network traffic; (2) maintain sufficient records to support incident investigation (i.e., monitoring, collecting, and analyzing current and historical evidence); and (3) implement measures to minimize the likelihood of an attacker removing evidence of their Tactics, Techniques, and Procedures (TTPs)[57] from compromised devices. Logging, including packet capture, of network traffic is critical for a responsible entity to assess the

[56] Packet capture allows information to be intercepted in real-time and stored for long term or short-term analysis, this providing a network defender greater insight into a network. Packet captures provide context to security events, such as intrusion detection system alerts. *See* CISA, *National Cybersecurity Protection System Cloud Interface Reference Architecture, Volume 1, General Guidance*, at 13,25, (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_NCPS_Cloud_Interface_RA_Volume-1.pdf.

[57] TTPs describe the behavior of an actor. Tactics are high-level descriptions of behavior, techniques are detailed descriptions of behavior in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit. *See*, NIST, *NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing*, (Oct. 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

severity of the attack, assess the scope of systems compromised, and devise appropriate mitigations.

32. We seek comments on all aspects of the proposed directive, including the three objectives discussed above. In particular, we seek comments on: (1) what are the potential challenges to implementing INSM (e.g., cost, availability of specialized resources, and documenting compliance); (2) what capabilities (e.g., software, hardware, staff, and services) are appropriate for INSM to meet the security objectives described above; (3) are the security objectives for INSM described above necessary and sufficient and, if not sufficient, what are other pertinent objectives that would support the goal of a having responsible entities successfully implement INSM; and (4) what is a reasonable timeframe for expeditiously developing and implementing Reliability Standards for INSM given the importance of addressing this reliability gap?

2. Low Impact BES Cyber Systems

33. While our proposal is centered on high and medium impact BES Cyber Systems, we also seek comments on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low impact BES Cyber Systems, including any potential benefits, technical barriers and associated costs. In particular, we seek comments on whether the same risks associated with high and medium impact BES Cyber Systems apply to low impact BES Cyber Systems. Those risks could include: (1) escalating privileges; (2) moving inside the CIP networked environment (i.e. trust zone); and (3) executing unauthorized code. To the extent such risks exist, we seek

comment on the appropriate scope of coverage for INSM needed to meet the security objectives listed above for low impact BES Cyber Systems.

34. As discussed above, there may be benefits to having INSM requirements apply to a defined subset of low impact BES Cyber Systems. To better understand the potential benefits of such an approach, we first seek comment on possible criteria or methodology for identifying an appropriate subset of low impact BES Cyber Systems that could benefit from INSM. For example, should the subset focus on low impact BES Cyber Systems located at assets strategic for the reliable operation of the BES, such as control centers and backup control centers, transmission stations and substations, and/or generation resources. Second, we seek comment on the potential benefits or drawbacks of defining a subset of low impact BES Cyber Systems. For example, would focusing resources on the assets with a more significant risk profile within the broad low impact tier of BES Cyber Systems improve an entity's risk profile and avoid situations where an attacker exploits legitimate cyber resources without timely detection and response. Third, as discussed above, there are currently no CIP requirements for low impact BES Cyber Systems for monitoring communications at the ESP.[58] Would it make sense to require INSM when perimeter monitoring is not required? Would it be appropriate to address both perimeter monitoring and INSM for low impact BES Cyber Systems?

[58] *See supra* Para. 7.

III. Information Collection Statement

35. The information collection requirements contained in this Notice of Proposed Rulemaking are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[59] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[60] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this rule will not be penalized for failing to respond to this collection of information unless the collection of information displays a valid OMB control number. Comments are solicited on the Commission's need for the information proposed to be reported, whether the information will have practical utility, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques.

36. The proposal to direct NERC to develop new, or to modify existing, reliability standards (and the corresponding burden) are covered by, and already included in, the existing OMB-approved information collection FERC-725 (Certification of Electric Reliability Organization; Procedures for Electric Reliability Standards; OMB Control

[59] 44 U.S.C. 3507(d).

[60] 5 CFR 1320.11 (2021).

No. 1902-0225),[61] under Reliability Standards Development.[62] The reporting requirements in FERC-725 include the ERO's overall responsibility for developing Reliability Standards, such as any Reliability Standards that relate to internal network security monitoring for high and medium impact BES Cyber Systems.

IV. Environmental Analysis

37. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect on the human environment.[63] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[64] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Analysis

[61] Another item for FERC-725 is pending review at this time, and only one item per OMB Control No. can be pending OMB review at a time. In order to submit this NOPR timely to OMB, we are using FERC-725(1B) (a temporary, placeholder information collection number).

[62] Reliability Standards Development as described in FERC-725 covers standards development initiated by NERC, the Regional Entities, and industry, as well as standards the Commission may direct NERC to develop or modify.

[63] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

[64] 18 CFR 380.4(a)(2)(ii) (2021).

38. The Regulatory Flexibility Act of 1980 (RFA)[65] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

39. We are proposing only to direct NERC, the Commission-certified ERO, to develop modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for high and medium impact BES Cyber Systems.[66] Therefore, this Notice of Proposed Rulemaking will not have a significant or substantial impact on entities other than NERC. Consequently, the Commission certifies that this Notice of Proposed Rulemaking will not have a significant economic impact on a substantial number of small entities. Any Reliability Standards proposed by NERC in compliance with this rulemaking will be considered by the Commission in future proceedings. As part of any future proceedings, the Commission will make determinations pertaining to the Regulatory Flexibility Act based on the content of the Reliability Standards proposed by NERC.

V. Comment Procedures

40. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative

[65] 5 U.S.C. 601-612.

[66] *Cf. Cyber Security Incident Reporting Reliability Standards*, Notice of Proposed Rulemaking, 82 FR 61499 (Dec. 28, 2017), 161 FERC ¶ 61,291 (2017) (proposing to direct NERC to develop and submit modifications to the NERC Reliability Standards to improve mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES).

proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. Comments must refer to Docket No. RM22-3-000, and must include the commenter's name, the organization they represent, if applicable, and address in their comments. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

41. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's website at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software must be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

42. Commenters that are not able to file comments electronically may file an original of their comment by USPS mail or by courier-or other delivery services. For submission sent via USPS only, filings should be mailed to: Federal Energy Regulatory Commission, Office of the Secretary, 888 First Street, NE, Washington, DC 20426. Submission of filings other than by USPS should be delivered to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

VI. Document Availability

43. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the

contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov). At this time, the Commission has suspended access to the Commission's Public Reference Room due to the President's March 13, 2020 proclamation declaring a National Emergency concerning the Novel Coronavirus Disease (COVID-19).

44. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

45. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at 202-502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202)502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

(S E A L)

Debbie-Anne A. Reese,
Deputy Secretary.

Document Content(s)

RM22-3-000.docx.....1