182 FERC ¶ 61,021
DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM22-3-000; Order No. 887]

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

(Issued January 19, 2023)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule

SUMMARY: The Federal Energy Regulatory Commission (Commission) is directing the North American Electric Reliability Corporation (NERC) to develop and submit within 15 months of the effective date of this final rule for Commission approval new or modified Reliability Standards that require internal network security monitoring within a trusted Critical Infrastructure Protection networked environment for all high impact bulk electric system (BES) Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. In addition, the Commission directs NERC to perform a study of all low impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems without external routable connectivity, as set forth in the final rule, and to submit its study report to the Commission within 12 months of the issuance of this final rule.

DATES: This rule is effective **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

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

Leigh Faugust (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6396
leigh.faugust@ferc.gov

Seth Yeazel
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6890
seth.yeazel@ferc.gov

SUPPLEMENTARY INFORMATION:

182 FERC ¶ 61,021
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

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

ORDER NO. 887

FINAL RULE

(Issued January 19, 2023)

TABLE OF CONTENTS

Paragraph Numbers

I. Introduction ..... 1.
II. Background ..... 7.
A. Section 215 and the Mandatory Reliability Standards ..... 7.
B. Internal Network Security Monitoring ..... 8.
C. Notice of Proposed Rulemaking ..... 13.
III. Need for Reform ..... 18.
IV. Discussion ..... 23.
A. Overview ..... 23.
B. INSM for High and Medium Impact BES Cyber Systems ..... 31.
1. Comments ..... 32.
2. Commission Determination ..... 48.
C. INSM for Low Impact BES Cyber Systems ..... 59.
1. Comments ..... 61.
2. Commission Determination ..... 67.
D. Security Objectives ..... 69.
1. Comments ..... 70.
2. Commission Determination ..... 76.
E. Standards Development Timeframe ..... 80.
1. Comments ..... 81.

2. Commission Determination ..... 85.
F. NERC Study and Report on INSM Implementation ..... 87.
V. Information Collection Statement ..... 91.
VI. Environmental Analysis ..... 96.
VII. Regulatory Flexibility Act ..... 97.
VIII. Document Availability ..... 100.
IX. Effective Date and Congressional Notification ..... 103.

I. Introduction

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission directs the North American Electric Reliability Corporation (NERC) to develop new or modified Critical Infrastructure Protection (CIP) Reliability Standards that require internal network security monitoring (INSM) for CIP-networked environments for all high impact bulk electric system (BES) Cyber Systems[2] with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.[3] Further, the Commission directs NERC to submit a report within 12

[1] 16 U.S.C. 824o(d)(5) (The Commission may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.).

[2] BES Cyber Systems are defined as "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks." *See* 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. BES Cyber Systems are categorized 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. 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 impact 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).

[3] NERC defines external routable connectivity as 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." *See* NERC Glossary.

months of issuance of this final rule that studies the feasibility of implementing INSM at all low impact BES Cyber Systems[4] and medium impact BES Cyber Systems without external routable connectivity (i.e., BES Cyber Systems not subject to the new or revised Reliability Standards)[5].

2. INSM is a subset of network security monitoring that is applied within a "trust zone,"[6] such as an electronic security perimeter.[7] For the purpose of this rule, the trust zone applicable to INSM is the CIP-networked environment. INSM enables continuing visibility over communications between networked devices within a trust zone and detection of malicious activity that has circumvented perimeter controls. Further, INSM facilitates the detection of anomalous network activity indicative of an attack in progress,

[4] For ease of reference, low impact BES Cyber Systems include those with and without external routable connectivity.

[5] For ease of reference, BES Cyber Systems not subject to the new or revised Reliability Standards in this final rule will be referred to as all low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity.

[6] The U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) defines trust zone 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." 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.

[7] An electronic security perimeter is "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." NERC Glossary.

thus increasing the probability of early detection and allowing for quicker mitigation and recovery from an attack.

3. We find that, while the CIP Reliability Standards require monitoring of the electronic security perimeter and associated systems for high and medium impact BES Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This presents a gap in the currently effective CIP Reliability Standards. To address this gap, we direct NERC to develop new or modified CIP Reliability Standards requiring INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack.

4. As discussed below, while the Commission's Notice of Proposed Rulemaking (NOPR)[8] in this proceeding proposed to direct NERC to address INSM for all high and medium impact BES Cyber Systems, we are persuaded by commenters that raised certain concerns with the NOPR proposal and, in this final rule, limit our directive to all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.

---

[8] *See Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Notice of Proposed Rulemaking, 87 FR 4173 (Jan. 27, 2022), 178 FERC ¶ 61,038, at P 31 (2022) (INSM NOPR).

5. While NERC has flexibility in developing the content of INSM requirements, the new or modified CIP Reliability Standards must address the specific concerns that we identify in this final rule. In particular, in this final rule, we direct NERC to develop new or modified CIP Reliability Standards that are forward-looking, objective-based, and that address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment. 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. And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by: (1) logging network traffic (we note that packet capture is one means of accomplishing this goal);[9] (2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the

[9] While the NOPR stated that "any new or modified CIP Reliability Standards should address the ability to support operations and response by requiring responsible entities to . . . log and packet capture network traffic," *id.* (citation omitted), we clarify in this final rule that "packet capture" is one example of how to support that goal. Packet capture allows information to be intercepted in real-time and stored for long-term or short-term analysis, thus 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 24, 2020), https://www.cisa.gov/sites/default/files/publications/CISA_NCPS_Cloud_Interface_RA_Volume-1.pdfhttps://www.cisa.gov/sites/default/files/publications/CISA_NCPS_Cloud_Interface_RA_Volume-1.pdf.

likelihood of an attacker removing evidence of their tactics, techniques, and procedures[10] from compromised devices.[11]

6. We also direct NERC to submit the new or modified CIP Reliability Standards for Commission approval within 15 months of the effective date of this final rule. We believe that a 15-month deadline provides sufficient time for NERC to develop responsive standard(s) within NERC's standards development process.

7. Further, the Commission sought comment in the NOPR on the possible implementation of INSM to detect malicious activity in networks with low impact BES Cyber Systems but did not propose to direct the development of Reliability Standards for INSM for low impact BES Cyber Systems. In this final rule, we direct NERC to conduct a study to support future Commission actions to extend INSM requirements to all low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity. Specifically, NERC should include in its study 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

[10] NIST defines tactics, techniques, and procedures as describing the behavior of an actor, where "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." NIST further explains that "tactics, techniques, and procedures 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*, at 2 (Oct. 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[11] INSM NOPR, 178 FERC ¶ 61,038 at P 31.

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. We believe that this information would provide the basis for further Commission action, as warranted, regarding INSM or alternatives. We direct NERC to file its study report with the Commission within 12 months of the issuance of this final rule.

II. Background

A. Section 215 and the Mandatory Reliability Standards

8. FPA section 215 provides that the Commission may certify an Electric Reliability Organization (ERO), the purpose of which is to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[12] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[13] Pursuant to FPA section 215, the Commission established a process to select and certify an ERO[14] and subsequently certified NERC.[15]

---

[12] 16 U.S.C. 824o(c).

[13] 16 U.S.C. 824o(e).

[14] *Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, & Enf't of Elec. 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).

[15] *N. Am. Elec. 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).

B. Internal Network Security Monitoring

9. INSM 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. INSM consists of three stages: (1) collection; (2) detection; and (3) analysis. Taken together, these three stages provide the benefit of early detection and alerting of intrusions and malicious activity.[16] Some of the tools that may be used for INSM include: anti-malware; intrusion detection systems; intrusion prevention systems; and firewalls.[17] 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.[18] This 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

---

[16] *See* Chris Sanders & Jason Smith, *Applied Network Security Monitoring*, at 9-10 (Nov. 2013); *see also* ISACA, *Applied Collection Framework: A Risk-Driven Approach to Cybersecurity Monitoring* (Aug. 18, 2020), https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/applied-collection-framework.

[17] *See* NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, at 10-13 (July 2013), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf.

[18] SANS Institute, *Applying Security Awareness to the Cyber Kill Chain* (May 31, 2019), https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/.

of the entity's systems, and carrying out the attack (e.g., exfiltration of project files, administrator credentials, and employee personal identifiable information). Thus, successful cyberattacks require the attacker to: (1) gain access to a target system; and (2) execute commands while in that system.

11. INSM could better position an entity to detect malicious activity that has circumvented perimeter controls and gained access to the target system. 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 and expected network activity and determine whether observed anomalous activity warrants further investigation.[19] The recorded network traffic can also be retained to facilitate timely recovery and/or perform a thorough post-incident analysis of malicious

[19] *See* CISA, *Best Practices for Securing Election Systems*, Security Tip (ST19-002) (Aug. 25, 2021), https://www.cisa.gov/tips/st19-002.

activity. 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 reporting and response; and (3) analyzing the attack itself to inform actions to prevent it from happening again.[20]

13. In summary, INSM better positions 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, 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. Finally, INSM provides insight into east-west network traffic[21] happening inside the network perimeter, which enables a more

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

[21] East-west traffic refers to the communications among BES Cyber Systems and is the specific type of network traffic that remains within the network perimeter. It may refer to communication peer-to-peer industrial automation and control systems devices in a network or to activity between servers or networks inside a data center, rather than the data and applications that traverse networks to the outside world. CISCO, *Networking and Security in Industrial Automation Environments Design Guide*, at 111 (Aug. 2020), https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Horizontal/DG/Industrial-AutomationDG.pdf; The President's National Security Telecommunications Advisory Committee, *Report to the President on Software-Defined Networking*, at E-3 (Aug. 12, 2020), https://www.cisa.gov/sites/default/files/publications/NSTAC%20SDN%20Report%20%288-12-20%29.pdf.

comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone.[22]

C. Notice of Proposed Rulemaking

14. On January 20, 2022, the Commission issued the INSM NOPR proposing to direct NERC to develop new or modified CIP Reliability Standards to require INSM for high and medium impact BES Cyber Systems. In the NOPR, the Commission preliminarily found that the currently effective CIP Reliability Standards do not address INSM, thus leaving a gap in the CIP Reliability Standards.[23] The NOPR explained that including INSM requirements in the CIP Reliability Standards would ensure that responsible entities maintain visibility over communications between networked devices within a trust zone rather than simply monitoring communications at the network perimeter access point(s) (i.e., at the boundary of an electronic security perimeter as required by the current CIP requirements).[24]

15. The NOPR discussed various risks to trusted CIP networks posed by the lack of requirements for INSM in the Standards, which include attackers: (1) escalating privileges; (2) moving inside the CIP-networked environment; and (3) executing

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

[23] INSM NOPR, 178 FERC ¶ 61,038 at PP 2, 14, 26.

[24] *Id.* PP 2, 26.

unauthorized code.[25] In the context of supply chain risk, the NOPR explained that 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.[26] The NOPR explained that, because the CIP-networked environment is a trust zone, a 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. Further, in the context of an insider threat, an employee with elevated administrative credentials could identify and collect data, add accounts, delete logs, or even exfiltrate data without being detected. The NOPR also pointed to the SolarWinds attack as an example of how an attacker can bypass all network perimeter-based security controls traditionally used to identify the early phases of an attack.[27] This supply chain attack leveraged a trusted vendor to compromise the networks of public and private organizations.[28]

[25] *Id*. P 33

[26] *Id*. P 17.

[27] *Id*. P 18 (citing 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).

[28] A threat actor gained access to the SolarWinds production environment, "pushed" malicious code through legitimate updates to customers and enabled the adversary to gain remote access and network privileges allowing the actor to manipulate identity and authentication mechanisms. *SolarWinds and Related Supply Chain Compromise* at 7.

16. The NOPR sought comments on all aspects of the proposed directive, and it also specifically solicited responses to the following questions: (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 necessary or appropriate for INSM to meet the security objectives; (3) are the three security objectives for INSM described in the NOPR necessary and sufficient and, if not sufficient, what are other pertinent objectives that would support the goal of having responsible entities successfully implement INSM; and (4) what is a reasonable timeframe for developing and implementing Reliability Standards for INSM.[29]

17. While the Commission's proposed directives centered on high and medium impact BES Cyber Systems, the Commission also sought comment on the usefulness and practicality of implementing INSM to detect malicious activity in networks with low impact BES Cyber Systems, as well as potentially identifying a subset of low impact BES Cyber Systems to which INSM requirements could apply.[30] In particular, the Commission sought comment on whether the same risks associated with high and medium impact BES Cyber Systems also apply to low impact BES Cyber Systems.[31] Commensurate with their impact on the Bulk-Power System, low impact BES Cyber

[29] INSM NOPR, 178 FERC ¶ 61,038 at P 32.

[30] *Id*. PP 4, 33-34.

[31] *Id*. P 33.

Systems have fewer security controls and, unlike high and medium impact BES Cyber Systems, are not subject to monitoring at the network perimeter access point(s).[32]

18. The comment period for the NOPR ended on March 28, 2022, and the Commission received 22 sets of comments, including one late-filed comment.[33] A list of commenters appears in Appendix A.

III. Need for Reform

19. INSM is a component of a comprehensive cybersecurity strategy as it provides an additional layer of defense against intrusions regardless of the attack vector or whether existing security controls failed. With INSM, an entity can maintain visibility over communications between networked devices within a trust zone and detect malicious activity that has circumvented perimeter controls.[34] INSM facilitates the detection of anomalous network activity indicative of an attack in progress, thus increasing the probability of early detection and allowing for quicker mitigation and recovery from an

[32] *See Version 5 Critical Infrastructure Protection Reliability Standards,* Order No. 791, 78 FR 72756 (Dec. 13, 2013), 145 FERC ¶ 61,160, at P 106 (2013), *order on clarification and reh'g*, Order No. 791-A, 78 FR 24107 (Apr. 24, 2013), 146 FERC ¶ 61,188 (2014) (finding that categorizing assets as high, medium, or low based on their impact on the reliable operation of the Bulk-Power System, with all BES Cyber Systems being categorized as at least low impact, offers more comprehensive protection than prior versions of the standards and declining to require NERC to develop specific controls for low impact facilities).

[33] The late-filed comment raised issues that were outside the scope of this rulemaking. Accordingly, we do not address the comment here.

[34] INSM NOPR, 178 FERC ¶ 61,038 at P 11.

attack.[35] Without INSM, an attacker may be able to move among devices internal to a trust zone using network pathways and required protocols to send malicious communications. Further, without INSM, an attacker could exploit legitimate cyber resources to: (1) escalate privileges (i.e., exploit a software vulnerability to gain administrator account privileges); (2) move undetected inside the trust zone of the CIP-networked environment; or (3) execute unauthorized code (e.g., a virus or ransomware).

20. Currently, network security monitoring in the CIP Reliability Standards focuses on network perimeter defense and preventing unauthorized access at the electronic security perimeter. While the CIP Reliability Standards require monitoring of inbound and outbound internet communications at the electronic security perimeter,[36] the currently effective CIP Reliability Standards do not require INSM *within* trusted CIP-networked environments for BES Cyber Systems. This leaves a gap in the CIP Reliability Standards for situations where vendors or individuals with authorized access are considered secure and trustworthy but could still introduce a cybersecurity risk, as well as other attack vectors that can exploit this gap. Additionally, the lack of INSM controls diminishes an essential component of a defense-in-depth strategy and therefore may increase the

[35] *Id.* P 2.

[36] *See* Reliability Standard CIP-005-6 (Electronic Security Perimeter(s)).

time it takes an entity to detect an intrusion and the time an attacker has to leverage compromised user accounts and traverse unmonitored network connections.[37]

21. The currently effective CIP Reliability Standards, while offering a broad set of cybersecurity protections, do not require INSM. For example, Reliability Standard CIP-005-6 (Electronic Security Perimeter(s)), Requirement R1.5 addresses monitoring of network traffic for malicious communications at the electronic security perimeter. Under CIP-005-6 Requirement R1.5, the only locations that require network security monitoring are the electronic security perimeter electronic access points for high and medium impact BES Cyber Systems at control centers. Additionally, 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 R.4.1.3, responsible entities must install security monitoring tools at the device level but are not required to use INSM methods, such as intrusion detection systems.[38]

---

[37] INSM NOPR, 178 FERC ¶ 61,038 at P 31; *see also* Nat'l Sec. Agency, *Network Infrastructure Security Guide* (June 2022), https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF.

[38] 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 only at the perimeter of all medium and high impact BES Cyber Systems (and not within the trust zone, unlike

22. Further, the currently effective CIP Reliability Standards do not require responsible entities to ensure that anomalous activity within the trust zone can be identified with a high level of confidence because the CIP Reliability Standards are focused on perimeter-based security with limited internal security controls. The three INSM security objectives—pertaining to (1) baselining, (2) monitoring and detecting unauthorized activity, and (3) identification of anomalous activity—aim to address this deficiency. As discussed below, new or modified Reliability Standards responsive to this final rule must address these three objectives.

23. For the reasons discussed below, in this final rule we affirm the preliminary finding in the NOPR that the lack of INSM requirements in the currently effective CIP Reliability Standards constitutes a security gap. Further, we conclude that there is a sufficient basis for a directive to NERC to require INSM in the CIP Reliability Standards for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.[39]

INSM). The related Measures for this provision provide examples of acceptable evidence of compliance, including a paper or system-generated listing of monitored activities for which the BES Cyber System is configured to log and capable of detecting.

[39] INSM architecture generally relies on external routable connectivity to achieve the full, real-time benefits of INSM, such as the capability to transmit collected data from network traffic and devices to a centralized location for further analysis by cybersecurity professionals.

IV. Discussion

A. Overview

24. Pursuant to FPA section 215(d)(5), we direct NERC to develop new or modified CIP Reliability Standards that require applicable responsible entities to implement INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. Given the importance of timely addressing the identified security gap, we direct that NERC submit responsive new or modified CIP Reliability Standards within 15 months of the effective date of this final rule. Based on the comments received in response to the NOPR, we determine that the record in this proceeding supports the development of mandatory requirements for the implementation of INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity that are within the control of responsible entities that fall within the scope of our authority under FPA section 215.

25. Overall, commenters agree with the benefits of implementing INSM as an additional layer of cybersecurity protection, although commenters differ on the contours of a directive to NERC to address the issue. NERC notes that while there may be challenges, INSM "would be an appropriate approach" to address the risks identified in the NOPR.[40]

[40] NERC Comments at 3; *see also* EPSA Comments at 3; Idaho Power Comments at 2; ISO/RTO Comments at 3.

26. NERC and other commenters support new or modified CIP Reliability Standards that address INSM for high impact BES Cyber Systems as a worthwhile improvement to the cybersecurity posture of the Bulk-Power System.[41] While no entities altogether oppose INSM for high impact BES Cyber Systems, two commenters recommend limiting INSM at high impact BES Cyber Systems to those located in a control center or those systems with external routable connectivity.[42]

27. Support for requiring the implementation of INSM for medium impact BES Cyber Systems varies, with a majority of commenters agreeing that extending INSM to at least some medium impact BES Cyber Systems could address the risks to the security of the Bulk-Power System identified in the NOPR.[43] Several other commenters also recognize that the NOPR's proposed directives regarding INSM are appropriate to address the threats that high and medium impact BES Cyber Systems face, and their potential impact on the reliable and secure operation of the Bulk-Power System.[44] Other commenters,

[41] *E.g.*, NERC Comments at 8; BPA Comments at 1; Trades Comments at 1.

[42] *See* ITC Comments at 7; Idaho Power Comments at 2.

[43] NERC Comments at 3; Consumers Comments at 1-2; Cynalytica Comments at 1; ISO/RTO Council Comments at 2-3; Juniper Comments at 1-2; Microsoft Comments at 1; MRO NSRF Comments at 1-2; NAGF Comments at 1; Nozomi Networks Comments at 3; OT Coalition Comments at 3; TAPS Comments at 14; Conway Comments at 1.

[44] *E.g.*, EPSA Comments at 3; Idaho Power Comments at 2; ISO/RTO Comments at 3.

however, either oppose the proposal for medium impact BES Cyber Systems[45] or advocate for delayed or limited inclusion of medium impact BES Cyber Systems within the scope of CIP Reliability Standards.[46]

28. Commenters raise challenges that may arise during development and implementation of CIP Reliability Standards requiring INSM for medium impact BES Cyber Systems that do not have external routable connectivity. These challenges include the large number of such medium impact BES Cyber Systems, which pose staffing and resource constraints for responsible entities and the possibility of supply chain constraints limiting the availability of necessary hardware and software tools to fully implement INSM.[47] As discussed below, we are persuaded by the comments raising challenges and thus modify the NOPR proposal by directing that NERC develop new or modified Reliability Standards requiring implementation of INSM for medium impact BES Cyber Systems with external routable connectivity.

29. Further, we decline at this time to direct NERC to develop new or modified CIP Reliability Standards to require INSM for low impact BES Cyber Systems. NERC and most other commenters note that the risks associated with high and medium impact BES Cyber Systems do not apply to low impact BES Cyber Systems and that the costs

[45] BPA Comments at 2.

[46] EPSA Comments at 2; Idaho Power Comments at 2; Indicated Trade Associations Comments at 9.

[47] *E.g.*, BPA Comments at 3; EPSA Comments at 3; Idaho Power Comments at 2.

associated with implementing INSM for low impact BES Cyber Systems would not result in a corresponding benefit to security.[48]

30. Although we decline to direct NERC to develop new or modified CIP Reliability Standards requiring INSM for medium impact BES Cyber Systems without external routable connectivity and all low impact BES Cyber Systems in this final rule, we recognize the importance of bolstering the cybersecurity of these systems. We believe that the current lack of visibility at low impact BES Cyber Systems, as well as medium impact BES Cyber Systems with similar configurations (i.e., serial-connected and other physical non-internet protocol based industrial control system communications), may leave systems vulnerable to cyberattacks that degrade the reliable and secure operation of the Bulk-Power System. However, we also recognize that extending INSM requirements to all low impact BES Cyber Systems would be difficult to implement or audit, given that there is neither a requirement for entities to identify their low impact BES Cyber Systems on an individual basis nor a requirement for entities to identify an electronic security perimeter for their low impact BES Cyber Systems.[49] Therefore, as discussed below, we

[48] *E.g.*, NERC Comments at 8; BPA Comments at 4-5; MRO NSRF Comments at 4; NAGF Comments at 4.

[49] Reliability Standard CIP-003-8 (Security Management Controls), Requirement R2, requires that an entity with low impact BES Cyber Systems must implement a cybersecurity plan that includes elements specified in Attachment 1 of CIP-003-8. While entities must implement a plan that includes "electronic access controls," the NERC defined term "Electronic Security Perimeter" is not mentioned in Attachment 1.

direct NERC, pursuant to section 39.2(d) of the Commission's regulations,[50] to submit to the Commission a report discussing the results of the study assessing the risks, implementation challenges, and potential solutions for all low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity, within 12 months of the issuance of this final rule.

31. We address below the following issues raised in the NOPR and NOPR comments: (1) the need for INSM Reliability Standards for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with and without external routable connectivity; (2) the extension of INSM to all low impact BES Cyber Systems; (3) security objectives of the new or modified Reliability Standards; and (4) standard development and implementation timelines. Further, we address the need for further study to support future action as warranted to require INSM for medium impact BES Cyber Systems without external routable connectivity and all low impact BES Cyber Systems.

B. INSM for High and Medium Impact BES Cyber Systems

32. In the NOPR, the Commission proposed to direct NERC to develop new or modified CIP Reliability Standards requiring that responsible entities implement INSM for their high and medium impact BES Cyber Systems.[51] The Commission preliminarily

[50] 18 CFR 39.2(d) (the ERO shall provide the Commission such information as is necessary to implement section 215 of the FPA).

[51] INSM NOPR, 178 FERC ¶ 61,038 at PP 29, 31.

found that INSM, as a fundamental element of a zero-trust architecture,[52] should improve the cybersecurity posture of responsible entities with high and medium impact BES Cyber Systems.[53] The NOPR explained that the proposed directive centers on high and medium impact BES Cyber Systems to improve visibility within networks containing BES Cyber Systems whose compromise could have a significant impact on the reliable operation of the Bulk-Power System.[54] The NOPR sought 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.

1. Comments

a. Implementation of INSM for High Impact BES Cyber Systems

33. NERC, BPA, Consumers, Cynalytica, ISO/RTO Council, Juniper Networks, Microsoft, MRO NSRF, NAGF, Nozomi Networks, and Conway support the NOPR's efforts to require INSM for high impact BES Cyber Systems.[55] NERC states its support

[52] NIST defines zero-trust architecture as "[a] security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The [zero-trust] security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses." NIST, Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/zero_trust_architecture.

[53] INSM NOPR, 178 FERC ¶ 61,038 at P 30.

[54] *Id.* P 3.

[55] NERC Comments at 3; Consumers Comments at 1-2; Cynalytica Comments at 1; ISO/RTO Council Comments at 2-3; Juniper Networks Comments at 1-2; Microsoft

for INSM as an "appropriate approach for consideration" for high impact BES Cyber Systems.[56]

34. BPA recommends that the Commission limit its initial rulemaking to only high impact BES Cyber Systems.[57] BPA recognizes INSM as an important cybersecurity protection but recommends phased adoption of INSM and limiting the initial rulemaking to high impact BES Cyber Systems, due to the resources and length of time needed to make such changes to industrial control systems. BPA recommends that the Commission, in a future proceeding, explore whether INSM requirements should apply to remote medium and low impact facilities without external routable connectivity.[58]

35. Indicated Trade Associations and Idaho Power recommend limiting the NOPR's proposal for high impact BES Cyber Systems. Indicated Trade Associations explains that by prioritizing high impact BES Cyber Systems, responsible entities would be able to "gather operational experience with INSM technologies."[59] While Indicated Trade Associations support implementation of INSM for high impact BES Cyber Systems, they also ask the Commission to convene a forum prior to issuing any directive. Idaho Power

---

Comments at 1; MRO NSRF Comments at 1-2; NAGF Comments at 1; Nozomi Networks Comments at 1; Conway Comments at 1.

[56] NERC Comments at 8.

[57] BPA Comments at 1.

[58] *Id.* at 3.

[59] Indicated Trade Associations Comments at 9.

also tempers its support of the NOPR recommendations, emphasizing that its support of INSM within BES Cyber Systems is limited to those with external routable connectivity—although also noting that the majority of high impact BES cyber systems likely already have external routable connectivity.[60]

36. ITC's comments support limiting INSM to high impact BES Cyber Systems located in control centers because they have larger numbers of more diversely routed systems with greater external connectivity and therefore more access for an attacker to exploit.[61] According to ITC, additional focus on the prevention of electronic security perimeter breaches continues to be the most effective overall approach to improving the cybersecurity of responsible entities. ITC also cautions that implementing INSM as contemplated by the NOPR could cause congestion and potentially slow the reactions of operators, who must observe and respond quickly to system and customer needs.[62] Instead of INSM, ITC states that it and many other entities already employ hub-and-spoke architecture[63] for their electronic security perimeters to protect the BES Cyber Systems and BES Cyber Assets within them, which it asserts are inconsistent with (and in

[60] Idaho Power Comments at 2.

[61] ITC Comments at 2-3.

[62] *Id.* at 2.

[63] ITC explains that hub-and-spoke architecture uses many, relatively small, electronic security perimeters, each containing a small number of BES Cyber Systems and/or Assets that are often in close physical proximity to each other but using few connections between Cyber Assets and Systems within each electronic security perimeter. *Id.* at 4.

many cases, duplicative of) the NOPR proposed directives. Further, ITC explains that as its hub-and-spoke architecture uses few connections between BES Cyber Assets and BES Cyber Systems within each electronic security perimeter, monitoring of such "fixed, small-scale network traffic" provides little security benefit compared to the costs.[64] ITC recommends that the Commission consider other cybersecurity strategies like application whitelisting[65] for defense-in-depth, which it asserts provide comparable security to INSM.[66]

37. Indicated Trade Associations and NAGF both note that entities may not have the same internal networks or architectures and that some may have implemented network segmentation or micro-segmentation of their networks.[67] NAGF explains that applying a complex and costly INSM infrastructure may disincentivize the use of segmentation.[68]

---

[64] *Id.*

[65] Whitelisting, also referred to as allowlisting, allows only selected authorized programs to run, while all other programs are blocked from running by default. It is used to establish a baseline for authorized applications and file locations and prevents any action that departs from that baseline. *See* CISA, *Guidelines for Application Whitelisting*, (2013), https://www.cisa.gov/uscert/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf.

[66] ITC Comments at 6.

[67] Indicated Trade Associations Comments at 17; NAGF Comments at 2. Network segmentation is one way of improving security by dividing a larger network into multiple segments, which each act as their own small network.

[68] NAGF Comments at 2.

b. Implementation of INSM for Medium Impact BES Cyber Systems

38. NERC, Consumers, Cynalytica, ISO/RTO Council, Juniper Networks, Microsoft, MRO NSRF, NAGF, Nozomi Networks, and Conway support the NOPR's efforts to require INSM for medium impact BES Cyber Systems.[69]

39. NERC states that it supports the efforts to address the risks identified in the NOPR (such as a bad actor leveraging vendors or others with authorized access to a network to attack these systems) and agrees that INSM is an appropriate approach to address such risks.[70] NERC comments that INSM could benefit the CIP Reliability Standards as a "consistent means of gaining visibility and awareness" within an electronic security perimeter.[71] Furthermore, NERC recognizes "the importance of maturing security controls pertaining to zero-trust principles within Reliability Standards" and agrees with the NOPR that INSM would advance responsible entities' cybersecurity posture towards zero-trust architecture.[72] Both NERC and Conway explain that INSM ensures that there is monitoring of east-west endpoint to endpoint communications internal to the electronic

[69] NERC Comments at 3; Consumers Comments at 1-2; Cynalytica Comments at 1; ISO/RTO Council Comments at 2-3; Juniper Networks Comments at 1-2; Microsoft Comments at 1; MRO NSRF Comments at 1-2; NAGF Comments at 1; Nozomi Networks Comments at 1; Conway Comments at 1.

[70] NERC Comments at 3.

[71] *Id.* at 5.

[72] *Id.* at 6.

security perimeter.[73] ISO/RTO Council and MRO NSRF, also supporting the NOPR proposal, state that systems solutions for anomaly detection, such as east-west monitoring, allow for more efficient summarizing of data and identification of anomalies.[74]

40. NAGF supports the NOPR proposal and states that INSM will complement existing network security perimeter monitoring requirements for high and medium impact BES Cyber Systems through improved internal network communications visibility.[75] In support of the NOPR proposal, Consumers notes that it has already independently concluded that INSM warrants investment and has implemented INSM for most of its high and medium impact BES Cyber Systems within an electronic security perimeter.[76]

41. Comments from technology vendors support the NOPR's proposed directives to add INSM to the NERC CIP Reliability Standards. Cynalytica and Microsoft both point to INSM as being crucial to a zero-trust strategy.[77] Cynalytica further opines "that all

[73] NERC Comments at 4-5; Conway Comments at 2.

[74] ISO/RTO Council Comments at 4-5; MRO NSRF Comments at 2.

[75] NAGF Comments at 1.

[76] Consumers Comments at 2.

[77] Cynalytica Comments at 1; Microsoft Comments at 3 (asserting that the Commission's recommendations for implementation of INSM on BES Cyber Systems is a cybersecurity best practice and is consistent with a zero-trust security model and is consistent with the White House zero-trust strategy published in January 2022 (citing White House, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)).

BES Cyber Systems should be monitored to ensure the visibility and operational situational awareness that a true zero-trust strategy brings in support of critical infrastructure resiliency."[78] Microsoft also supports directing NERC to develop Reliability Standards that require INSM for high and medium impact BES Cyber Systems.[79] Nozomi and Juniper Networks also support the proposal, asserting that, given the increasingly sophisticated methods by which attackers gain access to critical systems, it is critical that entities move beyond protection of the electronic security perimeter and implement dynamic, persistent monitoring measures.

42. CDWR, Electricity Canada, the OT Coalition, Reclamation, and TAPs focus their comments on the effectiveness of using INSM to achieve cybersecurity goals rather than explicitly supporting or opposing the NOPR proposal to implement INSM for high and medium impact BES Cyber Systems.[80] For example, CDWR requests that the Commission consider whether directives necessary to provide an adequate level of reliability and security are also cost effective.[81] And Electricity Canada states that it

[78] Cynalytica Comments at 4.

[79] Microsoft Comments at 1.

[80] CDWR Comments at 4; Electricity Canada Comments at 2; OT Coalition Comments at 3-4; Reclamation Comments at 3; TAPS Comments at 1.

[81] CDWR Comments at 4.

agrees that INSM is an important part of an overall cybersecurity strategy when implemented at appropriate locations in a network.[82]

c. Limiting INSM for Medium Impact BES Cyber Systems Based on External Routable Connectivity.

43. Although the NOPR did not distinguish the proposed directive for medium impact BES Cyber Systems by risk, their location at control centers, or the existence of external routable connectivity, commenters raise the possibility of limiting INSM on those bases.

44. EPSA, supporting Indicated Trade Associations' request for the Commission to convene a forum prior to issuing any directive, argues that while high impact BES Cyber Systems are indisputably worthy of INSM measures, any new requirements imposed on medium impact locations should be commensurate with the risk posed by each individual location that could be compromised. Therefore, EPSA asserts that if the Commission does act before convening a forum, that it phase in new requirements based on risk, for example beginning with high impact BES Cyber Systems and only medium impact BES Cyber Systems at control centers. EPSA states that this phased implementation would allow entities to account for challenges while controlling costs and constraints.[83]

45. ITC and Indicated Trade Associations support INSM for medium impact BES Cyber Systems located at control centers. ITC asserts that the Commission could direct NERC to develop a Reliability Standard which requires INSM only for high and medium

[82] Electricity Canada Comments at 2.

[83] EPSA Comments at 4.

impact BES Cyber Systems within control centers to achieve a more balanced risk-to-cost outcome. According to ITC, controls centers generally do contain more diversely routed Cyber Systems with greater external connectivity beyond the electronic security perimeter, which provides more access for an attacker to exploit.[84] Further, as ITC explains, control centers' electronic security perimeters already require network monitoring that reduces the difficulty and expense of implementing INSM at these locations.[85] Similarly, while Indicated Trade Associations agree with the Commission that implementation of INSM may improve the security posture of entities owning or operating high impact BES Cyber Systems and "holds significant potential to increase grid visibility and capability of detecting and mitigating malicious activity,"[86] they propose limiting the implementation to high impact BES Cyber Systems and medium impact BES Cyber Systems located at control centers.[87]

46. Idaho Power states that it agrees with the Commission that implementing INSM at medium impact BES Cyber Systems, in particular those with external routable connectivity, is "justified and necessary for the threats these systems are facing."[88] Idaho Power explains that BES Cyber Systems with external routable connectivity provide an

[84] ITC Comments at 7.

[85] *Id.*

[86] Indicated Trade Associations Comments at 7.

[87] *Id.* at 2.

[88] Idaho Power Comments at 2.

additional remote attack vector which is not present in systems without it, and warns that if there is a requirement for INSM for systems that do not currently have external routable connectivity, entities may add external routable connectivity (and therefore an additional attack vector) in order to meet the INSM requirements.[89] Idaho Power recommends that, if the Commission were to require INSM at high and medium impact BES Cyber Systems, the Commission should limit the directive to BES Cyber Systems with external routable connectivity, since external routable connectivity is arguably needed to take full advantage of INSM.[90] Although BPA recommends implementing INSM initially only at high impact BES Cyber Systems, it states that if the Commission orders implementation at medium impact BES Cyber Systems as well, the Commission should limit the implementation to medium impact BES Cyber Systems with external routable connectivity.[91]

47. Commenters point out the following concerns if this final rule were to apply to all medium impact BES Cyber Systems, including those without external routable connectivity: (1) lengthy timelines for implementation;[92] (2) lack of external routable connectivity at many medium impact BES Cyber Systems, which is needed to effectively

[89] *Id.*

[90] *Id.*

[91] BPA Comments at 3.

[92] *Id.*

implement INSM;[93] (3) for large entities, the undertaking may be sizable given their wider footprint for monitoring and detecting;[94] (4) already limited personnel would be stretched thin and there may be a shortage of qualified staff;[95] and (5) costs would far exceed any potential cybersecurity benefit.[96]

48. In its comments opposing INSM for medium impact BES Cyber Systems, BPA explains that many medium impact BES Cyber Systems do not have external routable connectivity and that these systems therefore pose minimal risk to intrusion and do not strongly implicate the INSM objectives identified by the Commission.[97] Similar to BPA, Indicated Trade Associations assert that not all medium impact BES Cyber Systems have external routable connectivity and therefore conclude that without this attack surface, there is less to monitor.[98] Furthermore, Indicated Trade Associations argue that medium impact BES Cyber Systems without external routable connectivity do not contain the same risk, or pose the same potential impact, as medium impact BES Cyber Systems with

[93] *Id.* at 1, 3; Idaho Power Comments at 2.

[94] Indicated Trade Associations Comments at 10 (referring to large entities with multi-state footprints and several hundred physical locations).

[95] *Id.* at 2; EPSA Comments at 4; ITC Comments at 5; TAPS Comments at 4.

[96] ITC Comments at 4; TAPS Comments at 3-5.

[97] BPA Comments at 4.

[98] Indicated Trade Associations Comments at 9.

external routable connectivity because an attacker does not have a path to move beyond the local trust zone.[99]

2. Commission Determination

49. Pursuant to FPA section 215(d)(5), we direct NERC to develop new or modified CIP Reliability Standards that require INSM for CIP-networked environments for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. We determine that requirements to implement INSM as we direct in this final rule will fill a gap in the current suite of CIP Reliability Standards and improve the cybersecurity posture of the Bulk-Power System.[100] Specifically, a requirement for INSM that augments existing perimeter defenses will increase network visibility so that an entity may understand what is occurring in its CIP-networked environment and, thus, improve capability to timely detect potential compromises.[101] INSM also allows for the collection of data and analysis required to implement a defense strategy, improves an entity's incident investigation

[99] *Id.* at 9-10.

[100] *See*, *e.g.*, NERC Comments at 4-5 (current CIP Standards require "malicious communications monitoring at the Electronic Access Point on the [electronic security perimeter], not necessarily monitoring of activity of those who already have access to the network").

[101] *Id.* at 5 ("CIP Reliability Standards could benefit from consideration of internal network security monitoring requirements as a consistent means of gaining visibility and awareness within an [electronic security perimeter].").

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.

50. Moreover, the NOPR identified certain cyber-related risks that implementation of INSM could mitigate through early detection, such as a supply chain attack leveraging malicious updates from a known software vendor (i.e., SolarWinds attack) and ransomware attacks.[102] NERC and other commenters agree that INSM is an appropriate approach to address such risks.[103]

51. We disagree with ITC's rationale for opposing the NOPR proposal. In particular, we disagree with ITC's assertions that the NOPR proposals are an "overly aggressive implementation of" zero-trust architecture.[104] As explained in the NOPR, while INSM is a fundamental element of the zero-trust architecture, it is only one of many aspects.[105] Furthermore, ITC presents its statement that there would only be little monitoring INSM could perform of its fixed, small-scale network traffic, and thus provide ITC little benefit,[106] without further context or explanation. Additionally, we disagree with ITC's assertion that application whitelisting provides comparable security to INSM. Application whitelisting is a security tool implemented at the cyber asset level and does

[102] INSM NOPR, 178 FERC ¶ 61,038 at PP 17-19.

[103] *E.g.*, NERC Comments at 6; Juniper Comments at 1.

[104] ITC Comments at 2.

[105] INSM NOPR, 178 FERC ¶ 61,038 at P 30.

[106] ITC Comments at 5.

not monitor network traffic, which is the purpose of INSM. Therefore, application whitelisting and INSM are two distinct components of a defense-in-depth strategy and two distinct components of zero-trust architecture.

52. We are also not persuaded by ITC's objections to the NOPR proposal based on ITC's claims regarding the relative limited vulnerability of hub-and-spoke networks. A hub-and-spoke connection is bound on both sides by electronic security perimeters. Like any other BES Cyber Asset, the electronic access points of the hub and spoke configuration are addressed by the currently effective CIP Reliability Standards, but there is currently no required monitoring of network traffic *within* the hub and spoke electronic security perimeters. We disagree with ITC's assertion that hub-and-spoke architecture has lower risk because it uses few connections between Cyber Assets and Cyber Systems within each electronic security perimeter.[107] INSM is a cybersecurity capability that is indifferent to the architecture to which it is applied. INSM is intended to monitor east-west network traffic that does not traverse the access point. An architecture like hub-and-spoke is not a substitute for a cybersecurity capability like INSM.

53. Finally, we disagree with ITC's assertion that the "NOPR's approach is also inconsistent with the Commission's long-standing risk-based approach to reliability."[108] The security objectives proposed in the INSM NOPR are risk-based and objective.[109]

---

[107] *Id.* at 4.

[108] *Id.*

[109] INSM NOPR, 178 FERC ¶ 61,038 at P 31.

Furthermore, malicious actors that compromise BES Cyber Systems within an electronic security perimeter could have the opportunity to perform the same functions as an authorized user, which includes operation of the Bulk-Power System, as demonstrated by the Ukraine attacks referenced in the INSM NOPR.[110]

54. We are not persuaded by BPA's request to limit our directive to INSM for high impact BES Cyber Assets based on resource and timing concerns nor persuaded by ITC's assertion that INSM would lead to congestion. Rather, we believe that our decision to limit our directive at this time to those medium impact BES Cyber Assets with external routable connectivity strikes a proper balance between limited resources and the security benefits of INSM and adequately addresses BPA's concerns and that technical concerns are better addressed during NERC's standards drafting process or during the implementation of INSM. Similarly, NAGF and Indicated Trade Associations' concern that requiring INSM may discourage entities from using greater network segmentation to enhance security is a specific technical concern better raised and addressed during NERC's standards drafting process.

55. We agree with commenters that articulate the various benefits of INSM. NERC and other commenters state that INSM ensures that there is monitoring of east-west endpoint-to-endpoint communications internal to the electronic security perimeter.[111] Likewise, ISO/RTO Council and MRO NSRF explain that systems solutions for anomaly

[110] *Id.* P 21.

[111] NERC Comments at 4-5; Conway Comments at 2.

detection, such as east-west monitoring, allow for more efficient summarizing of data and identification of anomalies.[112] Accordingly, the record in this proceeding supports incorporating INSM requirements into the CIP Standards for high and medium impact BES Cyber Systems, as set forth in this final rule.

56. We are not persuaded by Indicated Trade Associations' and ITC's suggestions to limit application of INSM to high impact BES Cyber Systems and medium impact BES Cyber Systems located at control centers.[113] Limiting application of INSM to high impact BES Cyber Systems and medium impact BES Cyber Systems located at control centers would constitute too narrow an approach because the trust zone associated with medium impact BES Cyber Systems encompasses systems with a definitive potential to affect Bulk-Power System reliability. We are, however, persuaded by commenters to limit the scope of our directive with regard to medium impact BES Cyber Systems to those with external routable connectivity. Idaho Power argues that the presence of external routable connectivity is an appropriate limiting factor for the directive,[114] and BPA, while it recommends applying the directive only to high impact BES Cyber Systems, states that if the directive encompasses medium impact BES Cyber Systems then it should apply only to medium impact BES Cyber Systems with external routable

[112] ISO/RTO Council Comments at 4-5; MRO NSRF Comments at 2.

[113] ITC Comments at 7; Indicated Trade Associations Comments at 11.

[114] Idaho Power Comments at 2.

connectivity.[115] Control centers generally already have external routable connectivity and are thus encompassed by a directive to limit application of INSM for medium impact BES Cyber Systems on the basis of external routable connectivity. For these reasons, we believe that external routable connectivity is a preferable approach to targeting the application of INSM.

57. Although not addressed in the NOPR, multiple commenters raised concerns regarding the efficacy and practicality of requiring implementation of INSM for medium impact BES Cyber Systems that lack external routable connectivity.[116] Simply stated, external routable connectivity allows remote communication with a BES Cyber System through use of a high-speed internet service to send information over a network. Typically, external routable connectivity allows higher quality data to flow from the field devices at substations to a centralized location where cybersecurity professionals can perform further analysis.

58. Commenters explain that a system without external routable connectivity, while not risk-free, is less vulnerable to attack than systems with external routable connectivity.[117] Likewise, according to commenters, external routable connectivity is

[115] BPA Comments at 3.

[116] *Id.*; EPSA Comments at 2; Idaho Power Comments at 1; ITC Comments at 7; Indicated Trade Associations Comments at 11.

[117] BPA Comments at 4; Indicated Trade Associations Comments at 9; Idaho Power Comments at 2. Medium impact BES Cyber Systems that lack external routable connectivity remain vulnerable to insider threats and supply chain attacks.

necessary to achieve the full, real-time benefits of INSM.[118] In consideration of these concerns, we modify the NOPR proposal and direct NERC to develop new or modified CIP Reliability Standards that require INSM for medium impact BES Cyber Systems with external routable connectivity.

59. While we agree with commenters regarding the challenges with implementing INSM for medium impact BES Cyber Systems without external routable connectivity such as costs and stretching thin limited resources,[119] we continue to believe that, if these challenges can be adequately addressed, implementation of INSM for all medium impact BES Cyber Systems would improve the cybersecurity posture of the Bulk-Power System by allowing early detection and response to cyber intrusions in BES Cyber Systems. Although we decline Indicated Trade Associations' request to convene a forum to discuss INSM in the proceeding prior to a directive as the robust comments provide an adequate basis for this final rule, we are directing NERC to conduct a study that pertains, *inter alia*, to the challenges of, and solutions for, implementing INSM at medium impact BES Cyber Systems without external routable connectivity and all low impact BES Cyber Systems, as discussed in more detail below.

C. INSM for Low Impact BES Cyber Systems

60. In the NOPR, the Commission stated that its proposal centered on high and medium impact BES Cyber Systems but sought comment on the usefulness and

[118] *See, e.g.*, BPA Comments at 2; Idaho Power Comments at 2.

[119] *E.g.*, Indicated Trade Associations Comments at 10.

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.[120] Low impact BES Cyber Systems have fewer security controls and, unlike high and medium impact BES Systems, are not subject to monitoring at the network perimeter access point(s). The Commission particularly sought comment on whether the same risks associated with high and medium impact BES Cyber Systems apply to low impact BES Cyber Systems, including escalating privileges, moving inside the CIP-networked environment, and executing unauthorized code. The Commission further sought comment on the appropriate scope of coverage for INSM for low impact BES Cyber Systems, to the extent such risks exist.

61. The Commission suggested that there may be benefits to having INSM requirements apply to a defined subset of low impact BES Cyber Systems and sought comment on possible criteria or methodology for identifying an appropriate subset of low impact BES Cyber Systems that could benefit from INSM.[121] The Commission further pointed out that there are currently no CIP requirements for low impact BES Cyber Systems for monitoring communications at the electronic security perimeter and therefore asked: (1) whether it makes sense to require INSM while perimeter monitoring is not

[120] INSM NOPR, 178 FERC ¶ 61,038 at P 33.

[121] *Id.* P 34.

required; and (2) would it be appropriate to address both perimeter monitoring and INSM for low impact BES Cyber Systems.[122]

1. Comments

62. Technology solutions vendors Cynalytica, Microsoft, Nozomi Networks, and OT Coalition support extending INSM to low impact BES Cyber Systems.[123] Microsoft recommends directing the implementation of INSM for low impact BES Cyber Systems "to the maximum extent practicable."[124] Cynalytica and Microsoft comment that risks within low impact BES Cyber Systems are similar to those within higher impact systems.[125] Cynalytica, Microsoft, and Nozomi Networks all assert that requiring all BES Cyber Systems to implement INSM at this time would reduce cybersecurity risk and exposure.[126] Cynalytica is of the opinion that "all BES Cyber Systems should be monitored to ensure the visibility and operational situational awareness," as low impact BES Cyber Systems "could be used for operational intelligence gathering, capabilities testing, or could be used to pivot among internal systems."[127]

---

[122] *Id*.

[123] Cynalytica Comments at 4; Microsoft Comments at 1; Nozomi Networks Comments at 3; OT Coalition Comments at 3-4.

[124] Microsoft Comments at 1.

[125] Cynalytica Comments at 4; Microsoft Comments at 11.

[126] Cynalytica Comments at 4; Microsoft Comments at 1; Nozomi Networks Comments at 3.

[127] Cynalytica Comments at 4.

63. Microsoft elaborates that low impact BES Cyber Systems such as distributed energy resources, along with their increasing use, may increase the potential risks associated with low impact BES Cyber Systems.[128] Nozomi Networks recommends extending INSM to low impact BES Cyber Systems as a possible way to both improve their security risks and posture over time, as well as identify potential supply chain security issues.[129]

64. OT Coalition, supporting a phased implementation of INSM for low impact BES Cyber Systems, warns that failure to account for the risk of a low impact BES Cyber System "being used as a lateral attack vector is inexcusable."[130] OT Coalition recommends that INSM-related and perimeter monitoring requirements should be phased in over time, e.g., over the course of five years and moving from larger to smaller entities.

65. Other commenters, however, advocate against requiring INSM at low impact BES Cyber Systems at this time. NERC, BPA, MRO NSRF, and NAGF oppose requiring INSM for low impact BES Cyber Systems as part of this proceeding because of the extensive revisions to the CIP Reliability Standards that would be needed and the

[128] Microsoft Comments at 11.

[129] Nozomi Networks Comments at 3.

[130] OT Coalition Comments at 4.

correspondingly longer time such revisions would take to implement.[131] For example, NERC and MRO NSRF point to the lack of any current requirement for a list of low impact BES Cyber Systems.[132] NERC and MRO NSRF also note that there is no current requirement for low impact BES Cyber Systems to have an electronic security perimeter.[133] Thus, according to MRO NSRF, to properly enact INSM at facilities with low impact BES Cyber Systems would require upgrading all such facilities to one with the same network architecture, protections, and monitoring as that of a facility with high or medium BES Cyber Systems and that the "cost and effort associated with such an enterprise would not be justified."[134]

66. NERC, BPA, CDWR, Consumers, EPSA, Idaho Power, MRO NSRF, NAGF, TAPS, Conway, and Indicated Trade Associations all caution that extending INSM requirements to low impact BES Cyber Systems at this time would be infeasible or impractical from a cost, time, and technical standpoint.[135] Indicated Trade Associations,

---

[131] NERC Comments at 8; BPA Comments at 4-5; MRO NSRF Comments at 4; NAGF Comments at 4.

[132] NERC Comments at 8-9; MRO NSRF Comments at 4 ("Analysis requires not just a monitoring system but a baseline inventory of BES Cyber Assets to have something to benchmark against.").

[133] *Id*.

[134] MRO NSRF Comments at 4.

[135] NERC Comments at 8-9; BPA Comments at 4-5; CDWR Comments at 4; Consumers Comments at 2; EPSA Comments at 4-5; Idaho Power Comments at 2-3; MRO NSRF Comments at 4; NAGF Comments at 4; TAPS Comments at 4-9; Conway Comments at 1; Indicated Trade Associations Comments at 28.

BPA, EPSA, TAPS, and CDWR explain that the sheer number of low impact BES Cyber Systems, which far exceeds that of medium and high impact BES Cyber Systems, makes implementation of INSM at low impact BES Cyber Systems impractical at this time, from a cost and time commitment perspective.[136] Reclamation notes that low impact BES Cyber Systems pose inherently less risk and therefore may not benefit from INSM as much as medium and high impact BES Cyber Systems.[137] NERC and other commenters explain that procuring the necessary support equipment, such as relays, remote terminal units, and communications processors, would be prohibitively expensive due to issues such as limited bandwidth, remote proximity of the systems, and greater variety of communications protocols.[138] NERC states that expanding INSM requirements to apply to low impact BES Cyber Systems would also pose scalability and manageability issues, such as considering whether communications paths would need to be enhanced to correct any latency or real-time operations impact.[139]

67. NAGF and Consumers assert that requiring INSM implementation for low impact BES Cyber Systems could displace efforts relating to higher impact systems.[140] TAPS

[136] BPA Comments at 4; CDWR Comments at 4; EPSA Comments at 4; TAPS Comments at 8; Indicated Trade Associations Comments at 28.

[137] Reclamation Comments at 3.

[138] NERC Comments at 8-9; Idaho Power Comments at 2-3; TAPS Comments at 5-6; Indicated Trade Associations Comments at 28.

[139] NERC Comments at 8-9.

[140] Consumers Comments at 2; NAGF Comments at 4.

comments that there are limited incremental reliability benefits due to low impact BES Cyber Systems being less likely to result in instability, uncontrolled separation, or cascading failure. TAPS further argues that there are technical barriers stemming from the diversity of low impact BES Cyber Systems requiring customized implementation and highly specialized staff.[141]

2. Commission Determination

68. We find comments explaining the challenges of extending INSM requirements to all low impact BES Cyber Systems are persuasive, and we therefore decline to direct NERC to extend requirements for INSM to all low impact BES Cyber Systems at this time. We agree with commenters such as Microsoft, Cynalytica, and Nozomi Networks that the risks within low impact BES Cyber Systems are similar to those within higher impact systems and that implementing INSM at low impact BES Cyber Systems would reduce cybersecurity risk and improve the overall security posture of the Bulk-Power System. Nevertheless, we are persuaded by NERC and other commenters that implementing INSM at all low impact BES Cyber Systems could present certain challenges that makes such a directive at this time impractical. We agree that extending INSM requirements to all low impact BES Cyber Systems could be difficult to scope, implement, or audit, given that there is no requirement for entities to individually identify their low impact BES Cyber Systems or electronic security perimeters for their low impact BES Cyber Systems. Additionally, we accept the explanation of NERC and other

[141] TAPS Comments at 3, 5.

commenters that extending INSM to low impact BES Cyber Systems could pose scalability and manageability issues,[142] pose challenges to limited company resources and specialization issues for locations with small support staff,[143] and require more highly specialized staff.[144]

69. Although declining to direct NERC at this time to do so, we believe that in the longer term it may be necessary that INSM be extended to at least some subset of low impact BES Cyber Assets to address the known risks associated with these assets. To address the challenges raised by commenters and support this goal, we direct NERC to study the hurdles and possible solutions of implementing INSM at all low impact BES Cyber Assets, as discussed below.

D. Security Objectives

70. In the NOPR, the Commission proposed that new or modified CIP Reliability Standards requiring INSM for high and medium impact BES Cyber Systems should address three security objectives pertaining to INSM.[145] First, any new or modified CIP Reliability Standards should address the need for each responsible entity to develop a baseline for their network traffic, specifically for security purposes. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to

[142] NERC Comments at 8-9.

[143] NAGF Comments at 4.

[144] TAPS Comments at 3, 5.

[145] INSM NOPR, 178 FERC ¶ 61,038 at P 31.

monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment. Third, any new or modified CIP Reliability Standards should address the ability to support operations and response by requiring responsible entities to ensure that anomalous activity can be identified to a high level of confidence by: (1) logging network traffic at a sufficient level of detail; (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.

1. Comments

71. Cynalytica characterizes the security objectives listed in the NOPR as a "solid foundation" and recommends that the CIP Reliability Standards adopt the objectives.[146] Microsoft, who strongly advocates for the implementation of the zero-trust security model, asserts that the security objectives from the NOPR align with this model and are critical to maintaining network visibility to drive threat detection and response in real time.[147] NAGF characterizes the security objectives listed in the NOPR as "acceptable and meaningful" and asserts that INSM will complement existing network perimeter monitoring requirements.[148]

[146] Cynalytica Comments at 3.

[147] Microsoft Comments at 2, 4.

[148] NAGF Comments at 1.

72. Specific to the security objectives proposed in the NOPR, commenters provide guidance for the development of a baseline of network traffic and suggest there could be alternative approaches. Electricity Canada asserts that there may be other approaches to analyzing network traffic besides baselining and suggests adopting "simplified language" that would not exclude the use of a type of technology based on the type of security analysis performed.[149] Electricity Canada recommends that the security objective should be to monitor for and detect unauthorized "network communication protocols," rather than unauthorized "software."[150]

73. Indicated Trade Associations explain that establishing a baseline of legitimate network traffic is challenging and calls for significant judgments unique to the implementation of INSM and that in this context baselining can have many different meanings.[151] According to Indicated Trade Associations, approaches to baselining could include: (1) simply differentiating between alerts and false positives as opposed to actual malicious activity; and (2) an expansive approach of fully mapping every packet between every asset on a network. Indicated Trade Associations states that the expenses and challenges of baselining increase if an expansive definition of baselining is adopted and recommends convening a forum to discuss and agree upon a workable definition.[152]

---

[149] Electricity Canada at 2.

[150] *Id.* at 3.

[151] Indicated Trade Associations Comments at 13-14.

[152] *Id.* at 14-15.

74. Conway urges that the Commission include in its security objectives language that focuses on desired operational capabilities, which Conway avers would help shape individual analyst roles and response actions and inform system operators and national response to information shared.[153] Conway explains that "[i]n order for the INSM . . . technologies to be meaningful or useful the sensors and implementation approach must be ICS [industrial control systems] protocol aware and provide detections."[154]

75. Beyond the proposed security objectives, multiple commenters generally support an objective, prioritized, flexible, and risk-based approach to the implementation of INSM to BES Cyber Systems. BPA and NAGF advocate for flexibility for the industry to develop risk-based criteria for implementation of INSM to allow entities to focus on their most important assets first and then consider whether other assets should be protected in the same manner.[155] ISO/RTO Council and MRO NSRF emphasize that any new or modified CIP reliability standards should allow registered entities the necessary flexibility to implement the INSM solution most appropriate for their own environments.[156]

76. Commenters suggest other security objectives that the Commission and NERC should prioritize. For example, NAGF suggests an objective of maintaining logs and

---

[153] Conway Comments at 4.

[154] *Id.* at 2.

[155] BPA Comments at 5; NAGF Comments at 4.

[156] ISO/RTO Council Comments at 4-5; MRO NSRF Comments at 2.

records of network activities.[157] Microsoft recommends that the Commission include a security objective to ensure that the operator has the staff and procedures in place to drive cybersecurity improvements from its INSM solution.[158] Microsoft explains that effective INSM implementation requires trained staff with the ability to respond to a pre-defined set of alerts with the security operations center or the network operations center. Microsoft further recommends a security objective requiring an intrusion detection system to perform threat vector analysis for assets on the network, to aid security personnel in prioritizing patching targets in its critical systems.[159]

2. Commission Determination

77. We agree with commenters that, as a general matter, the CIP Reliability Standards should be objective-based, technology neutral, and provide flexibility to entities in identifying how to address the three security objectives identified in the NOPR.

78. Regarding comments to include security objectives pertaining to adequate staffing and training, we believe that these goals are necessary to achieve the three objectives stated in the NOPR and need not be set out as separate objectives.[160] As described above, commenters raise a number of thoughts and suggestions pertaining to baselining, packet-

[157] NAGF Comments at 1.

[158] Microsoft Comments at 9-10.

[159] *Id.* at 10.

[160] *Id.* at 9-10.

level monitoring, logging, and capture of internal network traffic.[161] We expand our second security objective based on Electricity Canada's recommendation to replace software with network communication protocols by adding "network communication protocols" to the objective. However, we do not adopt other recommendations, because these matters are better raised during NERC's standards drafting process. We are not persuaded that such level of detail is useful to incorporate within the Commission's final rule. Instead, NERC's standards drafting process is the appropriate forum to determine the level of detail necessary to ensure the security objectives are met by any new or modified CIP Reliability Standards.

79. We direct NERC to ensure that the new or modified CIP Reliability Standards that require security controls for INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity address three security objectives for east-west network traffic. 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 network traffic and data flows for security purposes. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, network communication protocols, and software inside the CIP-networked environment, as well as encompass awareness of

[161] *See, e.g.*, Electricity Canada Comments at 2; EPSA Comments at 2-6; ISO/RTO Council Comments at 4-5; MRO NSRF Comments at 2; NAGF Comments at 1; Indicated Trade Associations Comments at 18-19.

protocols used in industrial control systems.[162] Third, in response to the comments requesting that any new or modified CIP Reliability Standards should be objective-based, we clarify our NOPR proposal so that it is not oriented toward specific technologies or activities, as discussed below.

80. We agree that any new or modified CIP Reliability Standards should provide flexibility to responsible entities in determining the best way to identify anomalous activity to a high level of confidence, so long as those methods ensure: (1) logging of network traffic (we note that packet capture is one means of accomplishing this goal); (2) maintaining those logs, and other data collected, regarding network traffic that are of sufficient data fidelity to draw meaningful conclusions and support incident investigation; and (3) maintaining the integrity of those logs and other data by implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures (maintaining the integrity of logs and other data assures an entity that analysis and findings from incident investigations are representative of the actual incident and can aid in the mitigation of current and future similar compromises).

E. Standards Development Timeframe

81. The Commission in the INSM NOPR requested comments on reasonable timeframes for expeditiously developing and implementing Reliability Standards for

[162] *E.g.*, Conway Comments at 2; CISA, *Industrial Control Systems Cybersecurity Initiative: Considerations for ICS/OT Monitoring Technologies with an Emphasis on Detection and Information Sharing*, at 2 (2021), https://www.cisa.gov/sites/default/files/publications/ICS-Monitoring-Technology-Considerations-Final-v2_508c.pdf.

INSM given the importance of addressing this reliability gap.[163] The INSM NOPR also inquired as to potential challenges to implementing INSM (e.g., cost, availability of specialized resources, and documenting compliance).

1. Comments

82. Among the few comments on the timeframe for developing new or modified standards addressing INSM, ISO/RTO Council suggests a one-to-two-year timeframe is appropriate.[164] NERC requests that, given the complexity of the subject matter, the Commission defer to NERC regarding the appropriate timeline for standards development to better assure that all relevant issues can receive the proper consideration in the standards development process.[165] Other commenters express caution, and counsel the Commission balance the competing needs of speed and quality in standards development.[166] Others suggest an iterative or staggered approach to standards development.[167]

83. Regarding timeframes for implementation of INSM (i.e., after the proposed INSM standards become effective), commenters recommend timeframes for implementation ranging from two to ten years, depending on whether INSM is to be extended to high

[163] INSM NOPR, 178 FERC ¶ 61,038 at P 32.

[164] ISO/RTO Council Comments at 3-6.

[165] NERC Comments at 3, 6-7.

[166] Reclamation Comments at 2; Cynalytica Comments at 3.

[167] NAGF Comments at 4; Conway Comments at 4.

impact, medium impact, or low impact BES Cyber Systems. Microsoft suggests a minimum of two years for applicable registered entities to come into compliance with a new INSM reliability standard based on typically budget cycles. Microsoft also points out that entities would need to change their networks to include INSM during a shutdown period, which occurs every 12 to 18 months.[168]

84. MRO NSRF and BPA aver that full implementation of INSM for high and medium impact BES Cyber Systems would require a minimum of three to five years, and MRO NSRF suggests a staggered implementation timeline.[169] MRO NSRF cites several challenges that could affect the implementation timeline, including: (1) supply chain constraints if multiple entities are trying to obtain INSM tools in the same timeframe; (2) shortages of qualified staff; and (3) higher cost due to additional requirements, system configurations, and sudden increase in demand.[170] MRO NSRF did not provide specific cost estimates.

85. Indicated Trade Associations do not provide a specific period but mention that implementing INSM for large entities would require a sizable undertaking, because doing so would entail installing new or upgraded network equipment, increasing network

[168] Microsoft Comments at 10.

[169] MRO NSRF Comments at 3; BPA Comments at 3.

[170] MRO NSRF Comments at 1-2.

connectivity, and installing multiple INSM monitoring devices requiring aggregation to provide complete operating pictures or baselines.[171]

2. Commission Determination

86. We direct NERC to submit responsive new or modified CIP Reliability Standards within 15 months of the effective date of this final rule. We believe that a 15-month deadline would provide sufficient time for NERC to develop responsive new or modified Standards within NERC's standards development process. This deadline is within the range of ISO/RTO Council's suggested one-to-two-year timeframe. Regarding NERC's request that the Commission not set a deadline, we believe that most of the complexities cited by NERC are resolved by our decision not to extend INSM in this final rule to low impact BES Cyber Systems and medium impact BES Cyber Systems without external routable connectivity.

87. We decline to direct a specific implementation timeframe for any new or modified standards. Commenters provide a wide range of potential implementation timeframes and raise concerns regarding resource availability and the need for flexibility in implementing new or modified INSM Reliability Standards. Rather than setting the implementation timeframe at this time, we believe NERC should propose an implementation period by balancing the various concerns raised by commenters as well as the need to timely address the identified gap in the CIP Standards pertaining to INSM.

[171] Indicated Trade Associations Comments at 10.

When submitting the proposed CIP Standards, NERC should provide its rationale for the chosen implementation timeframe.

F. NERC Study and Report on INSM Implementation

88. While determining above that it is premature to require INSM for medium impact BES Cyber Systems without external routable connectivity and all low impact BES Cyber Systems, we recognize the importance of bolstering the cybersecurity of those systems. We believe that extending INSM to all medium impact BES Cyber Systems and at least a subset of low impact BES Cyber Systems in the future could be necessary to protect the security and the reliability of the Bulk-Power System. To provide a basis for such action, we direct NERC, pursuant to section 39.2(d) of the Commission's regulations,[172] to conduct a study to guide the implementation of INSM, or other mitigation strategies, for medium impact BES Cyber Systems without external routable connectivity and all low impact BES Cyber Systems. The study shall focus on two main topics: (1) risk and (2) challenges and solutions.

89. First, regarding risk, NERC should collect from registered entities information on the number of low impact and medium impact BES Cyber Systems that would not be subject to the new or revised Reliability Standards, which would inform the scope of the risk from systems without INSM. Next, NERC should provide an analysis regarding the substantive risks posed by these BES Cyber Systems operating without the implementation of INSM. Specifically, NERC should determine the quantity of: (1)

[172] 18 CFR 39.2(d).

substation and generation locations that contain medium impact BES Cyber Systems without external routable connectivity; (2) low impact locations (including a breakdown by substations, generations resources, and control centers) that contain low impact BES Cyber Systems without external routable connectivity; and (3) low impact locations that contain low impact BES Cyber Systems with external routable connectivity (including a breakdown by substations, generations resources, and control centers). NERC should then discuss the risks to the security of the Bulk-Power System due to the lack of an INSM requirement for the identified facilities.

90. Second, regarding challenges and solutions, NERC should identify the potential technological, logistical, or other challenges involved in extending INSM to additional BES Cyber Systems, as well as possible alternative actions to mitigate the risk posed. For example, as discussed in more detail above, challenges raised by commenters include: (1) lengthy timelines for identifying the location of low impact BES Cyber Systems; (2) the need to add external routable connectivity at many medium impact BES Cyber Systems to effectively implement INSM; (3) a wider footprint for monitoring and detecting for larger entities; (4) shortages of qualified staff; and (5) supply chain constraints.

91. NERC should consult with Commission staff to ensure that the study adequately addresses the topics discussed above. We direct NERC to submit the study report to the Commission within 12 months of the issuance of this final rule.

V. Information Collection Statement

92. The information collection requirements contained in this order are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995. OMB's regulations require approval of certain information collection requirements imposed by agency rules. 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.

93. The reporting requirements (and associated burden) proposed by the NOPR in Docket No. RM22-3-000 are already covered by the OMB-approved FERC-725. However, we are seeking clearance for this collection of information under FERC-725(1B), which is a temporary placeholder number. FERC-725(1B) is being used because FERC-725 (OMB Control Number 1902-0225) is pending review at OMB for another collection of information, and only one item per OMB control number can be pending review at a time. Otherwise, the collection of information for this final rule would be submitted to OMB under FERC-725, as discussed in the NOPR, since the

reporting requirements and associated burdens in this final rule are already covered by FERC-725.

94. This final rule requires that entities that are in the NERC Compliance Registry have an obligation to respond to the Commission directed NERC study, and thus there is a burden to be included in FERC-725(1B) information collection requirements.

95. The NERC Compliance Registry, as of October 3, 2022, identifies approximately 1,682 utilities, both public and non-public, in the U.S. that may respond to the NERC study. For the following reasons, we are using placeholders of one respondent, one response, and one burden hour for FERC-725(1B) in order to submit this request to OMB for PRA review.

1) We anticipate that the collection of information in this final rule will become part of FERC-725 when that collection becomes available for revision.
2) FERC-725 already includes burdens associated with the ERO's responsibility for Reliability Standards Development
3) In order to submit the collection of information in this final rule, we must submit it through the ROCIS system, which requires figures for respondents, responses, and burdens.

96. To approximate NERC's cost for the temporary, placeholder FERC-725(1B), we are using the estimated average of $91/hour (for wages and benefits) for 2022 for a Commission employee. Therefore, the estimated annual cost of the one placeholder burden hour is $91.

VI. Environmental Analysis

97. 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.[173] 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.[174] The actions directed herein fall within this categorical exclusion in the Commission's regulations.

VII. Regulatory Flexibility Act

98. The Regulatory Flexibility Act of 1980 (RFA)[175] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities.

99. By only proposing to direct NERC, the Commission-certified ERO, to develop modified Reliability Standards for INSM at BES Cyber Systems, this final rule will not

[173] *Reguls. Implementing the Nat'l Env't. Pol'cy Act*, Order No. 486, 52 FR 47897 (Dec. 17, 1987), FERC Stats. & Regs. Preambles 1986-1990 ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

[174] 18 CFR 380.4(a)(2)(ii).

[175] 5 U.S.C. 601-612.

have a significant or substantial impact on entities other than NERC.[176] Therefore, the Commission certifies that this final rule will not have a significant economic impact on a substantial number of small entities.

100. 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.

VIII. Document Availability

101. 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).

102. 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.

103. User assistance is available for eLibrary and the FERC's website during normal business hours from FERC Online Support at 202-502-6652 (toll free at 1-866-208-3676)

[176] *See, e.g.*, *Cyber Sec. Incident Reporting Reliability Standards*, Order No. 848, 83 FR 36727 (July 31, 2018), 164 FERC ¶ 61,033, at P 103 (2018).

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.

IX. Effective Date and Congressional Notification

104. These regulations are effective [insert date 30 days from publication in Federal Register for non-major rules and 60 days from the later of the date Congress receives the agency notice or the date the rule is published in the Federal Register]. The Commission has determined, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in § 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

By the Commission.

(S E A L)

Debbie-Anne A. Reese,
Deputy Secretary.

Note: the following Appendix will not appear in the *Code of Federal Regulations.*

Appendix
Commenters

Abbreviation	Commenter
BPA	Bonneville Power Administration
CDWR	California Department of Water Resources State Water Project
Consumers	Consumers Energy Company
Conway	Tim Conway
Cynalytica	Cynalytica, Inc.
Electricity Canada	Electricity Canada
Entergy	Entergy
EPSA	Electric Power Supply Association
Idaho Power	Idaho Power Company
Indicated Trade Associations	Edison Electric Institute, the American Public Power Association, the Large Public Power Council, the National Rural Electric Cooperative Association, and the Electric Power Supply Association
ISO/RTO Council	ISO/RTO Council
ITC	International Transmission Company
Juniper Networks	Juniper Networks
Microsoft	Microsoft Corporation
MRO NSRF	Midwest Reliability Organization NERC Standards Review Forum
NAGF	North American Generator Forum
NERC	North American Electric Reliability Corporation, Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.
Nozomi Networks	Nozomi Networks
OT Coalition	Operational Technology Cybersecurity Coalition
Reclamation	United States Bureau of Reclamation
TAPS	Transmission Access Policy Study Group