188 FERC ¶ 61,175
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM24-7-000]

Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring

(Issued September 19, 2024)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to approve proposed Reliability Standard CIP-015-1 (Cyber Security – Internal Network Security Monitoring), which the North American Electric Reliability Corporation (NERC), submitted in response to a Commission directive. In addition, the Commission proposes to direct that NERC develop certain modifications to proposed Reliability Standard CIP-015-1 to extend internal network security monitoring to include electronic access control or monitoring systems and physical access control systems outside of the electronic security perimeter.

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

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

- Electronic Filing: Documents must be filed in acceptable native applications and

print-to-PDF, but not in scanned or picture format.

- For those unable to file electronically, comments may be filed by USPS mail or by hand (including courier) delivery.
    - Mail via U.S. Postal Service Only: Addressed to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, N.E., Washington, DC 20426.
    - Hand (including courier) delivery: Deliver to: Federal Energy Regulatory Commission, 12225 Wilkins Avenue, Rockville, MD 20852.

The Comment Procedures Section of this document contains more detailed filing procedures.

FOR FURTHER INFORMATION CONTACT:

Margaret Steiner (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502 6704
Margaret.Steiner@ferc.gov

Hampden T. Macbeth (Legal Information)
Office of General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502 8957
Hampden.Macbeth@ferc.gov

SUPPLEMENTARY INFORMATION:

188 FERC ¶ 61,175
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring — Docket No. RM24-7-000

NOTICE OF PROPOSED RULEMAKING

(Issued September 19, 2024)

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission proposes to approve proposed Critical Infrastructure Protection (CIP) Reliability Standard CIP-015-1 (Cyber Security – Internal Network Security Monitoring). The North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization (ERO), submitted the proposed Reliability Standard for Commission approval in response to a Commission directive in Order No. 887.[2] In addition, pursuant to section 215(d)(5) of the FPA,[3] the Commission proposes to direct that NERC develop further modifications to Reliability Standard CIP-015-1, within 12 months of the effective date of a final rule in this proceeding, to extend Internal Network Security Monitoring (INSM)[4] to include electronic access control or monitoring systems

[1] 16 U.S.C. 824o(d)(2).

[2] *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Order No. 887, 88 FR 8354 (Feb. 9, 2023), 182 FERC ¶ 61,021 (2023).

[3] 16 U.S.C. 824o(d)(5).

[4] INSM is "a subset of network security monitoring that is applied within a 'trust zone,' such as an electronic security perimeter." Order No. 887, 182 FERC ¶ 61,021 at

(EACMS)[5] and physical access control systems (PACS)[6] outside of the electronic security perimeter.

2. In Order No. 887, the Commission directed that NERC develop new or modified CIP Reliability Standards that require INSM for CIP-networked environments for all high impact bulk electric system (BES) Cyber Systems[7] with and without external routable connectivity[8] and medium impact BES Cyber Systems with external routable

---

P 2.

[5] EACMS are "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." NERC, *Glossary of Terms Used in NERC Reliability Standards*, (July 22, 2024), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (NERC Glossary).

[6] PACS are "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." *Id.*

[7] NERC defines BES Cyber Systems as "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." *See* NERC Glossary. 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).

[8] External routable connectivity is "[t]he 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." NERC Glossary.

connectivity.[9] Proposed Reliability Standard CIP-015-1 is partly responsive to the Commission's directives in Order No. 887 and advances the reliability of the Bulk-Power System by (1) establishing requirements for INSM for network traffic inside an electronic security perimeter, and (2) 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 identification of anomalous network activity indicating an ongoing attack.[10] Accordingly, we propose approving proposed Reliability Standard CIP-015-1.

3. Proposed Reliability Standard CIP-015-1 is not, however, fully responsive to the Commission's directive to implement INSM for the "CIP-networked environment."[11] In particular, the proposed Standard may not adequately defend against attacks that circumvent network perimeter-based security controls. Attacks external to the electronic security perimeter may compromise systems, such as EACMS or PACS, and then infiltrate the perimeter as a trusted communication, thus limiting the effectiveness of an approach that employs INSM only within the electronic security perimeter. The Commission used the phrase "CIP-networked environment" in Order No. 887 to be necessarily broader than the electronic security perimeter.[12] Accordingly, to address this reliability and security gap, the Commission proposes to direct that NERC develop

[9] Order No. 887, 182 FERC ¶ 61,021 at P 49.

[10] NERC Petition at 1, 13.

[11] *See* Order No. 887, 182 FERC ¶ 61,021 at P 1.

[12] *Id.* P 49.

modifications to the proposed Reliability Standard CIP-015-1 to extend INSM to include EACMS and PACS outside of the electronic security perimeter.

I. Background

A. Section 215 and Mandatory Reliability Standards

4. Section 215 of the FPA provides that the Commission may certify an ERO, the purpose of which is to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval.[13] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[14] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[15] and subsequently certified NERC.[16]

B. Internal Network Security Monitoring

5. INSM is a subset of network security monitoring that is applied within a "trust zone,"[17] such as an electronic security perimeter. The trust zone applicable to INSM is

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

[14] *Id.* 824o(e).

[15] *Rules Concerning Certification of the Elec. Reliability Org.; & Procs. for the Establishment, Approval, & Enforcement of Elec. Reliability Standards*, Order No. 672, 114 FERC ¶ 61,104, *order on reh'g*, Order No. 672-A, 114 FERC ¶ 61,328 (2006); *see also* 18 CFR 39.4(b) (2024).

[16] *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).

[17] 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*

the CIP-networked environment for this notice of proposed rulemaking (NOPR) and Order No. 887.[18] 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, thus increasing the probability of early detection and allowing for quicker mitigation and recovery from an attack.

6. 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.[19] 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

---

Connections 3.0: Reference Architecture, 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf.

[18] Order No. 887, 182 FERC ¶ 61,021, at P 2.

[19] *See* CHRIS SANDERS & JASON SMITH, APPLIED NETWORK SECURITY MONITORING, 9-10 (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.

insight into east-west network traffic[20] happening inside the network perimeter, which enables a more comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone.[21]

C. Order No. 887

7. On January 19, 2023, in Order No. 887, the Commission issued a final rule that directed that NERC 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."[22] The Commission, noting that INSM is "applied within a 'trust zone,' such as an electronic security perimeter," stated that for the final rule the applicable trust zone for INSM is the CIP-networked environment.[23]

---

[20] 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*, 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*, E-3 (Aug. 2020), https://www.cisa.gov/sites/default/files/publications/NSTAC%20SDN%20Report%20%288-12-20%29.pdf.

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

[22] Order No. 887, 182 FERC ¶ 61,021 at P 3.

[23] *Id.* P 2.

8. The Commission explained that the currently effective CIP Reliability Standards focus on preventing unauthorized access at the electronic security perimeter and do not require INSM inside trusted CIP-networked environments.[24] The Commission determined that this left a reliability gap when vendors or individuals with authorized access are deemed trustworthy but could still introduce a cybersecurity risk.[25] The Commission then concluded that requirements to implement ISNM will "fill a gap in the current suite of CIP Reliability Standards and improve the cybersecurity posture of the Bulk-Power System."[26]

9. The Commission directed that NERC ensure that the new or modified CIP Reliability Standards address three security objectives for east-west network traffic. First, the new or modified CIP Reliability Standards should address the need for each responsible entity to develop a baseline for their network activity by analyzing for security purposes their network traffic and data flows. Second, the new or modified CIP Reliability Standards should address the need for responsible entities to monitor and

[24] *Id.* P 20.

[25] *Id.* An attacker could move among devices inside a trust zone and perform actions such as: (1) escalate privileges (such as gaining administrator account privileges through a vulnerability); (2) move undetected inside the CIP-networked environment; or (3) execute a virus, ransomware or another form of unauthorized code. *Id.* P 19.

[26] *Id.* P 49 (citing NERC Comments in Response to Notice of Proposed Rulemaking under Docket No. RM22-3-000 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")). The Bulk-Power System is defined in the FPA as facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy. 16 U.S.C. 824o(a)(1).

detect "unauthorized activity, connections, devices, network communication protocols, and software" in the CIP-networked environment. Third, the new or modified CIP Reliability Standards should provide responsible entities with flexibility in determining how to best identify anomalous activity with a high level of confidence, so long as the methods ensure: (1) logging of network traffic; (2) maintaining the logs, and other data collected, regarding network traffic that are of "sufficient data fidelity to draw meaningful conclusions" to investigate an incident; and (3) maintaining the integrity of the logs and other data by employing measures that minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures.[27]

D. NERC Petition and Proposed Reliability Standard CIP-015-1

10. On June 24, 2024, NERC submitted for Commission approval proposed Reliability Standard CIP-015-1 and the associated violation risk factors and violation severity levels, implementation plan, and effective date.[28] NERC states that proposed Reliability Standard CIP-015-1 is intended to advance the reliability of the Bulk-Power System by providing a comprehensive suite of forward looking and objective-based requirements for INSM.[29]

[27] Order No. 887, 182 FERC ¶ 61,021 at PP 79-80.

[28] NERC Petition at 2, 26-28. Proposed Reliability Standard CIP-015-1 is not attached to this NOPR. The proposed Reliability Standards are available on the Commission's eLibrary document retrieval system in Docket No. RM24-7-000 and on the NERC website, www.nerc.com.

[29] *Id.* at 4.

11. NERC explains that the proposed Reliability Standard would address the directives in Order No. 887 by establishing three requirements for responsible entities to implement INSM systems and processes. Specifically:

- Requirement R1: responsible entities would be required to implement process(es) to monitor, detect, and evaluate anomalous activity in "networks protected by the Responsible Entity's Electronic Security Perimeter(s)" of high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity.[30]
- Requirement R2: responsible entities would be required to implement process(es) for retaining INSM data associated with anomalous network activity as determined by the applicable responsible entities.
- Requirement R3: responsible entities would be required to implement process(es) to protect INSM monitoring data collected and retained in support of Requirements R1 and R2 to guard against the risk of unauthorized deletion or modification.

According to NERC, Requirement R1 applies to data flows within "networks protected by the Responsible Entity's Electronic Security Perimeter(s)."[31] NERC states that proposed Reliability Standard CIP-015-1's scope is consistent with the plain language of Order No. 887, which stated that INSM should apply within a trust zone, "such as an electronic security perimeter," and that the trust zone for INSM is the "CIP-networked

[30] *Id.*, Ex. A (Proposed Reliability Standard CIP-015-1) at 6.

[31] *Id.*

environment."[32] NERC states that its approach would provide the greatest benefits to the reliability of the Bulk-Power System by focusing industry's limited resources on the most critical environment, "networks protected by the Responsible Entity's Electronic Security Perimeter."[33]

II. Discussion

A. Proposal to Approve Proposed Reliability Standard CIP-015-1

12. Pursuant to section 215(d)(2) of the FPA, the Commission proposes to approve proposed Reliability Standard CIP-015-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. The proposed Reliability Standard requires responsible entities to implement INSM within the electronic security perimeter for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity. Consistent with the security objectives identified in Order No. 887, Requirement R1 of the proposed Standard would require responsible entities to implement INSM by mandating the collection, detection, analysis of and appropriate response to anomalous activity within the electronic security perimeter. Proposed Reliability Standard CIP-015-1, Requirement R2 would require responsible entities to retain INSM data related to anomalous activity. Proposed Reliability Standard CIP-015-1, Requirement R3 would require responsible entities to protect INSM data associated with anomalous network activity.

[32] NERC Petition at 16 (quoting Order No. 887, 182 FERC ¶ 61,021 at P 2).

[33] *Id.* at 14, 17.

13. Implementation of INSM within the electronic security perimeter will augment responsible entities' ability to detect anomalous or malicious activity and provide information to assist in determining an appropriate response through proposed Reliability Standard CIP-015-1, Requirements R1, R2, and R3. The proposed Reliability Standard improves the security posture of the industry by providing visibility into east-west communications absent from previous Reliability Standards, improving the probability of detection for anomalous or malicious activity within the electronic security perimeter.

14. Notwithstanding the improvements to security made by the proposed Standard, as discussed below, the proposed Reliability Standard does not fully implement the scope of protection contemplated in Order No. 887. By restricting the implementation of INSM to within the electronic security perimeter, a reliability and security gap remains by not implementing INSM for the entire CIP-networked environment, i.e., outside the electronic security perimeter inclusive of EACMS and PACS. To address this gap, we propose to direct NERC to develop modifications to the proposed Reliability Standard to include EACMS and PACS, thereby protecting the reliability and security of all trust zones of the CIP-networked environment. This approach—proposing to approve a Reliability Standard as enhancing protections and as a separate action under section 215(d)(5) of the FPA proposing to direct NERC to develop certain modifications to a Reliability Standard to address a reliability gap—is consistent with Commission precedent.[34]

[34] *See e.g., N. Am. Elec. Reliability Corp.*, 187 FERC ¶ 61,204 (2024) (order approving Reliability Standard EOP-012-2 because it clarified the requirements for generator cold weather preparedness and by making other improvements and, in addition,

B. Scope of the CIP-Networked Environment

15. NERC's proposed application of the term "CIP-networked environment" as limited to assets and systems within the electronic security perimeter is overly narrow. Order No. 887 used the term "CIP-networked environment" purposefully to apply more broadly than the electronic security perimeter, specifically to include all assets and systems to which the CIP standards apply and may be the targets of attacks. As explained below, NERC's petition does not address that reliability and security gap because it does not require implementation of INSM at EACMS and PACS outside the electronic security perimeter.

16. Excluding EACMS and PACS from the term "CIP-networked environment" is inconsistent with generally accepted approaches to cybersecurity. Under Reliability Standard CIP-002-5.1a and fundamental cybersecurity practices, similar systems within a network are grouped together to facilitate management, control, and monitoring of the networked environment.[35] For example, EACMS are grouped together to allow for early detection of malicious activity within the CIP-networked environment and potentially

---

directing that NERC submit modifications to Reliability Standard EOP-012-2 to address certain concerns); *Critical Infrastructure Prot. Reliability Standard CIP-012-1 – Cyber Sec. – Commc'ns between Control Ctrs.*, Order No. 866, 85 FR 7197 (Feb. 7, 2020), 170 FERC ¶ 61,031 (2020).

[35] Reliability Standard CIP-002.5.1a (BES Cyber System Categorization) (categorizing EACMS, PACS, protected cyber assets, and BES Cyber Systems into groups); *see, e.g.*, Nat'l Sec. Agency, *Network Infrastructure Security Guide*, 1, 3-4 (Oct. 2023), https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF (recommending the grouping of similar network systems as a best practice for overall network security) (NSA Network Security Guide).

protect other grouped systems, such as BES Cyber Systems, with which the EACMS communicate. Thus, excluding certain grouped systems from protections—as is the case for EACMS and PACS in Reliability Standard CIP-015-1—leaves other grouped systems within the CIP-networked environment at risk. Here, the BES Cyber Systems would not benefit from monitoring of east-west (i.e., lateral) movement within the grouping of EACMS and PACS, which allows for early detection of anomalous or malicious activity.[36] Otherwise, for example, a compromised EACMS grouping could provide an attacker with the opportunity to infiltrate other connected groups, such as BES Cyber Systems located within the electronic security perimeter, as an authenticated user or trusted communication.[37]

[36] *See* CISA, *Cybersecurity Advisory: CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks*, 2, 14 (Feb. 2023), https://www.cisa.gov/sites/default/files/2023-03/aa23-059a-cisa_red_team_shares_key_findings_to_improve_monitoring_and_hardening_of_networks.pdf (finding that insufficient network monitoring contributed to a CISA red team avoiding detection and gaining access to an organization's network through lateral movement by leveraging access to an Active Directory system serving as an electronic access control system) (CISA Cybersecurity Advisory); Nat'l Inst. of Standards and Tech. (NIST), *NIST SP 800-215 Guide to a Secure Enterprise Network Landscape*, 5 (Nov. 2022), https://doi.org/10.6028/NIST.SP.800-215 (describing the limitations of a perimeter-based security approach as not capturing threats from inside a network that can move laterally and remain undetected for an extended period of time) (NIST SP 800-215); NIST, *NIST SP 800-82r3 Guide to Operational Technology (OT) Security*, 74 (Sept. 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (recommending the analyzing of information to differentiate between known and unknown communication as a necessary first step in implementing network security monitoring) (NIST SP 800-82r3). The term INSM is used by the Commission in Order No. 887, but the cybersecurity industry uses the term "network security monitoring." Similarly, the CIP Standards use the terms "EACMS" and "PACS," which are defined by the NERC Glossary, while NIST discusses the same concepts but does not use the same EACMS and PACS terminology.

[37] *See* CISA Cybersecurity Advisory at 2-6 (describing how a CISA Red Team was able to gain access to workstations and servers from an Active Directory system

17. National Institute of Standards and Technology (NIST) guidance states that INSM monitoring needs to detect "[a]ny threat that is already inside of a network [that] can move laterally and remain undetected for days or even months."[38] According to the NIST guidance, east-west (lateral) monitoring (i.e., INSM) improves the probability of detection for malicious or anomalous activity and should not be isolated to only the most critical trust zones.[39] While the terminology of EACMS and PACS is unique to the CIP Reliability Standards, these statements from NIST broadly include the concepts of EACMS and PACS and support the need for monitoring.

18. Further, we find NERC's rationale for limiting INSM to within the electronic security perimeter unpersuasive. First, NERC contends that the devices supporting reliable operation are contained within the electronic security perimeter and thus industry resources are most effectively focused on data flows within the electronic security perimeter.[40] We disagree. While the devices *directly* supporting the reliable operation of the Bulk-Power System are located within the electronic security perimeter, attacks that threaten reliability can still emanate from outside the electronic security perimeter from connected Cyber Assets, such as EACMS.[41]

---

serving as an electronic access control system, which assisted in lateral movement to other networks).

[38] NIST SP 800-215 at 5.

[39] *See id.* (describing east-west traffic as "largely invisible to security teams" without INSM and that a threat inside a network can move east-west and "remain undetected for days or even months").

[40] NERC Petition at 14.

[41] *See, e.g.*, CISA Cybersecurity Advisory at 1-2 (a CISA Red Team was able to

19. Second, NERC avers that requiring INSM implementation outside the electronic security perimeter could have the unintended effect of impeding an entity's ability to detect and respond to threats to their most critical systems due to alarm and alert fatigue from large volumes of generated data.[42] Extending INSM implementation to include EACMS and PACS may generate large volumes of data;[43] however, we believe that the data can be managed and that the security benefits of implementing INSM outside the electronic security perimeter outweigh the burden associated with increased volumes of data. Defining incident alerting thresholds and establishing a baseline for normal network activity can reduce the potential for alarm and alert fatigue.[44] Restricting INSM to the assets within the electronic security perimeter could leave the most critical networks vulnerable to an attack from outside the electronic security perimeter. Assets such as EACMS are high value targets for an attack because if successfully compromised, EACMS would allow an attacker to infiltrate the perimeter as a trusted

---

gain access to systems adjacent to the organization's sensitive business systems (SBSs) by moving laterally from workstations and servers through an Active Directory system; Phase I of the attack ended before the team could implement a viable plan to achieve access to a SBS).

[42] NERC Petition at 14-15 n.45.

[43] *See* NIST SP 800-82r3 at 130 (discussing alert "noise" from typical network traffic that can result from implementation of network security monitoring).

[44] *See id.* at 127-128 (recommending that organizations define incident alert thresholds to establish an efficient incident detection capability as not all events and anomalies are malicious or require investigation and establish alerting thresholds on baselines of normal network traffic and data flows to reduce false positive and nuisance alarms).

communication.[45] Further, declining to extend INSM implementation to EACMS and PACS outside the electronic security perimeter leaves a reliability gap because responsible entities will lack visibility into the high percentage of east-west traffic that occurs within the CIP-networked environment.[46] Monitoring and alerting of east-west traffic enables quicker detection of malicious communications, minimizing potential harmful effects.[47] Additionally, the collected data serves as invaluable forensic evidence in the event of an attempted or successful compromise of the CIP-networked environment.

20. Third, NERC asserts that requiring INSM implementation outside the electronic security perimeter would not promote security and reliability inside the CIP-networked environment or that the cost of doing so would outweigh associated benefits.[48] We disagree. EACMS and PACS are integral to the effective operation of BES Cyber Systems within the electronic security perimeter in providing services, such as centralized authentication, authorization, and monitoring, and serving as the access point to the electronic security perimeter.[49] These assets are valued targets for an attacker and

[45] *See, e.g.*, CISA Cybersecurity Advisory at 14 (finding a CISA red team gained access to an organization's network due to the lack of monitoring on endpoint management systems – high valued assets – that can include the monitoring system part of an EACMS).

[46] NIST states that over 75% of network traffic is now east-west or server-to-server, i.e., traffic that is not covered by a perimeter-based defense approach. *See* NIST SP 800-215 at 5.

[47] *See id.* at 5.

[48] NERC Petition at 15-16 n.46.

[49] NERC, *Lessons Learned: CIP Version 5 Transition Program* (Sept. 2015),

illustrate the need for a defense-in-depth strategy for cybersecurity.[50] Implementing INSM outside the electronic security perimeter provides significant benefits in monitoring, detecting, and collecting malicious code or anomalous activity from attackers moving east-west within the EACMS or PACS network segments of the CIP-networked environment and is a fundamental cybersecurity practice.[51]

C. Proposed Directive

21. Pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to proposed Reliability Standard CIP-015-1 that would extend INSM to include EACMS and PACS outside the electronic security perimeter. We also propose directing NERC to submit the revised Reliability Standard for Commission approval within 12 months of the effective date of a final rule in this proceeding. We seek comment on all aspects of this proposal.

III. Information Collection Statement

22. The FERC-725B information collection requirements 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 will not be penalized for failing to respond to these

https://www.nerc.com/pa/CI/tpv5impmntnstdy/LL_EACMS_Mixed_Trust_Authentication_Sep_10_2015_clean.pdf.

[50] *See, e.g.*, CISA Cybersecurity Advisory at 2-6, 14.

[51] *See* NIST SP 800-215 at 5; NSA Network Security Guide at 3.

collections of information unless the collections of information display a valid OMB control number. The Commission solicits comments on the need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

23. The Commission bases its paperwork burden estimates on the additional paperwork burden presented by the proposed revision to Reliability Standard CIP-015-1 as this is a new proposed Reliability Standard. Reliability Standards are objective-based and allow entities to choose compliance approaches best tailored to their systems. The NERC Compliance Registry, as of July 2024, identifies approximately 1,636 unique U.S. entities that are subject to mandatory compliance with CIP Reliability Standards. Of this total, we estimate that 400 entities will face an increased paperwork burden under proposed Reliability Standard CIP-015-1. Based on these assumptions, we estimate the following reporting burden:

Annual Changes Proposed by the NOPR in Docket No.RM24-7-000[52]

[52] The paperwork burden estimate includes costs associated with the initial

	Number of Respondents (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[53] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
Create one or more documented process(es) (R1)	400	1	400	40 hrs.; $3,880	16,000 hrs.; $1,552,000	$3,880
Create documentation detailing network data feed(s) and reason (R1.1)	400	1	400	60 hrs.; $5,820	24,000 hrs.; $2,328,000	$5,820
Create documentation of: anomalous events and baseline used to	400	1	400	60 hrs.; $5,820	24,000 hrs.; $2,328,000	$5,820

development of a policy to address the requirements.

[53] This burden applies in Year One to Year Three.

The hourly cost for wages is based in part on the average of the occupational categories from the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm) plus benefits:

Legal (Occupation Code: 23-0000): $162.66

Electrical Engineer (Occupation Code: 17-2071): $79.31
Office and Administrative Support (Occupation Code: 43-0000): $48.59

($162.66 + $79.31 + $48.59) ÷ 3 = $96.85

The figure is rounded to $97.00 for use in calculating wage figures in this NOPR.

detect anomalous events (R1.2)						
Create documentation of methods to: evaluate anomalous activity; response to detected activity; and escalation process(es) (R1.3)	400	1	400	60 hrs.; $5,820	24,000 hrs.; $2,328,000	$5,820
Create documentation of: data retention process(es); system configuration(s), or system-generated report(s) (R2)	400	1	400	60 hrs.; $5,820	24,000 hrs.; $2,328,000	$5,820
Create documentation of how the collected data is being protected (R3)	400	1	400	60 hrs.; $5,820	24,000 hrs.; $2,328,000	$5,820

Total burden for FERC-725B(5) under CIP-015-1			2,400		136,000 hrs.; $13,192,000	$32,980

24. The responses and burden hours for Years 1-3 will total respectively as follows:

- Year 1-3 each: 2,400 responses; 136,000 hours
- The annual cost burden for each year One to Three is $13,192,000.

25. Title: Mandatory Reliability Standards, Revised Critical Infrastructure Protection Reliability Standards

Action: Revision to FERC-725B information collection.

OMB Control No.: 1902-0248.

Respondents: Businesses or other for-profit institutions; not-for-profit institutions.

Frequency of Responses: On Occasion.

Necessity of the Information: This NOPR proposes to approve the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission proposes to approve proposed Reliability Standard CIP-015-1 pursuant to section 215(d)(2) of the FPA because it improves upon the currently-effective suite of cybersecurity CIP Reliability Standards.

Internal Review: The Commission has reviewed the proposed Reliability Standard and made a determination that its action is necessary to implement section 215 of the FPA.

Interested persons may obtain information on the reporting requirements by contacting the following: Federal Energy Regulatory Commission, 888 First Street, NE Washington, DC 20426 [Attention: Kayla Williams, Office of the Executive Director, email: DataClearance@ferc.gov, phone: (202) 502-8663, fax: (202) 273-0873].

26. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-4638, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to: oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM24-7-000 and OMB Control Number 1902-0248.

IV. Environmental Analysis

27. 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.[54] 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

[54] *Reguls. Implementing the Nat'l Envtl Pol'y 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).

not substantially change the effect of the regulations being amended.[55] The action proposed herein falls within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Certification

28. The Regulatory Flexibility Act of 1980 (RFA)[56] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities. The Small Business Administration's (SBA) Office of Size Standards develops the numerical definition of a small business.[57] The SBA revised its size standard for electric utilities (effective March 17, 2023) to a standard based on the number of employees, including affiliates (from the prior standard based on megawatt hour sales).[58] The Commission believes that because the obligations imposed upon industry are directed at only entities that own or operate high impact BES Cyber Systems with or without external routable connectivity or medium impact BES Cyber Systems with external routable connectivity that there are no entities that meet the SBA revised standard for electric utilities. Therefore, the Commission certifies that this NOPR will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

[55] 18 CFR 380.4(a)(2)(ii).

[56] 5 U.S.C. 601-612.

[57] 13 CFR 121.101.

[58] 13 CFR 121.201, Subsector 221 (Utilities).

VI. Comment Procedures

29. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Comments must refer to Docket No. RM24-7-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

30. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

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

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

VII. Document Availability

33. 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).

34. 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.

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

By direction of the Commission.

Debbie-Anne A. Reese,
Acting Secretary.