This document is scheduled to be published in the
Federal Register on 07/02/2025 and available online at
https://federalregister.gov/d/2025-12309, and on https://govinfo.gov

7-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

18 CFR Part 40

[Docket No. RM24-7-000; Order No. 907]

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

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Final action.

SUMMARY: The Federal Energy Regulatory Commission (Commission) approves 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 directs NERC to 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. The Commission also provides greater clarity about the term CIP-networked environment as it is used in proposed Reliability Standard CIP-015-1.

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

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:

1. Pursuant to section 215(d)(2) of the Federal Power Act (FPA),[1] the Commission approves 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 proposed Reliability Standard CIP-015-1 for Commission approval in response to a Commission directive in Order No. 887.[2] In Order No. 887, the Commission directed that NERC develop new or modified CIP Reliability Standards that require internal network security monitoring (INSM)[3] for the CIP-networked environment for all high impact bulk electric system (BES) Cyber Systems[4] with and without external routable connectivity[5] and medium impact BES Cyber Systems with external routable connectivity.[6]

---

[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] INSM is a subset of network security monitoring that is applied within a trust zone, such as a perimeter zone with elevated credentials inside of an entity's internal network.

[4] 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 of Terms Used in NERC Reliability Standards*, (February 26, 2025), https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf (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).

[5] 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.

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

2. Consistent with Order No. 887, Reliability Standard CIP-015-1 improves upon the currently effective CIP Reliability Standards by establishing requirements for INSM for network traffic inside an electronic security perimeter. Reliability Standard CIP-015-1 requires 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.[7] Accordingly, the Commission approves Reliability Standard CIP-015-1 as it is largely responsive to the Commission's directives in Order No. 887 and will improve the security posture of the Bulk-Power System. We also approve the associated violation risk factors and violation severity levels, implementation plan, and effective date.

3. In Order No. 887, the Commission used the term CIP-networked environment to define the "trust zone" in which INSM requirements should apply.[8] The Commission, however, did not define the term CIP-networked environment in Order No. 887. Nor did NERC propose a definition in its petition. Rather, NERC and other commenters ask in Notice of Proposed Rulemaking (NOPR) comments that the Commission clarify the meaning of the term CIP-networked environment.[9]

4. We clarify that the term CIP-networked environment does not cover all of a responsible entity's network. The CIP-networked environment includes traffic inside an

---

[7] NERC Petition at 1, 13.

[8] *E.g.*, Order No. 887, 182 FERC ¶ 61,021 at P 2.

[9] *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring*, 89 FR 79178 (Sept. 27, 2024), 188 FERC ¶ 61,175 (2024) (NOPR).

electronic security perimeter but also extends beyond the perimeter. The CIP-networked environment includes the systems within the electronic security perimeter *and* network connections among and between electronic access control or monitoring systems (EACMS) [10] and physical access control systems (PACS) [11] external to the electronic security perimeter as discussed in greater detail below.[12] It is necessary to defend against attacks external to the electronic security perimeter because they may compromise systems such as EACMS and PACS, and then infiltrate the perimeter as a trusted communication. Thus, EACMS and PACS are included in the CIP-networked environment.

5. With this clarification, it is apparent that Reliability Standard CIP-015-1, which requires INSM only within the electronic security perimeter, is not fully compliant with the Commission's directive in Order No. 887. Therefore, pursuant to section 215(d)(5) of the FPA,[13] we direct NERC to develop further modifications to proposed Reliability Standard CIP-015-1, within 12 months of the effective date of the final rule in this proceeding, to extend INSM to include EACMS and PACS outside of the electronic security perimeter.

---

[10] 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.

[11] 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.*

[12] When we refer to EACMS and PACS in this final rule it also includes the network segments delineated in P 43, *infra*.

[13] 16 U.S.C. 824o(d)(5).

I. Background

A. Section 215 and Mandatory Reliability Standards

6. 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.[14] Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[15] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[16] and subsequently certified NERC.[17]

B. Internal Network Security Monitoring

7. INSM is a subset of network security monitoring that is applied within a trust zone,[18] such as a perimeter zone with elevated credentials inside of an entity's internal network. For this final rule and Order No. 887, the trust zone applicable to INSM is the

---

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

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

[16] *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); *see also* 18 CFR 39.4(b).

[17] *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).

[18] 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*, 2 (July 2020), https://www.cisa.gov/sites/default/files/publications/CISA_TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf.

CIP-networked environment.[19] 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.

8. 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.[20] 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 (i.e., lateral) network traffic[21] happening inside the network

---

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

[20] *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.

[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*, 111 (Aug. 2020), https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Industrial_Automation/IA_Ho

perimeter, which enables a more comprehensive picture of the extent of an attack compared to data gathered from the network perimeter alone.[22]

C. Order No. 887

9. 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."[23] 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.[24]

10. 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 the trusted CIP-networked environment.[25] The Commission determined that this left a reliability gap when vendors or individuals with authorized

---

rizontal/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.

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

[24] *Id.* P 2.

[25] *Id.* P 20.

access are deemed trustworthy but could still introduce a cybersecurity risk.[26] The Commission then concluded that requirements to implement INSM will "fill a gap in the current suite of CIP Reliability Standards and improve the cybersecurity posture of the Bulk-Power System."[27]

11. 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 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

---

[26] *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.

[27] *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).

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.[28]

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

12. 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.[29] NERC stated 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.[30]

13. NERC explained 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:

- 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.[31]

---

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

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

[30] *Id.* at 4.

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

- 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.

14. According to NERC, Requirement R1 applies to data flows within "networks protected by the Responsible Entity's Electronic Security Perimeter(s)."[32] NERC stated 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 environment.[33] NERC stated 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."[34]

E. Notice of Proposed Rulemaking

15. On September 19, 2024, the Commission issued a NOPR proposing to approve proposed Reliability Standard CIP-015-1 as just, reasonable, not unduly discriminatory or

---

[32] *Id.*

[33] *Id.* at 16 (quoting Order No. 887, 182 FERC ¶ 61,021 at P 2).

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

preferential, and in the public interest.[35] The NOPR stated that the three requirements of the proposed Reliability Standard aligned with the security objectives identified in Order No. 887.[36]

16. While proposing to approve proposed Reliability Standard CIP-015-1, the Commission also proposed to direct that NERC develop modifications to the Reliability Standard to address a reliability gap. Specifically, the Commission stated that proposed Reliability Standard CIP-015-1 does not fully implement the scope of protection contemplated in Order No. 887 because it limits INSM implementation to within the electronic security perimeter, instead of extending it to the entire CIP-networked environment.[37] To address this reliability gap, the Commission proposed to direct NERC to develop modifications to proposed Reliability Standard CIP-015-1 to include EACMS and PACS outside of the electronic security perimeter, thereby protecting the reliability and security of all trust zones of the CIP-networked environment.[38]

17. In response to the NOPR, five entities submitted comments: ISO/RTO Council (IRC); New England States Committee on Electricity (NESCOE); NERC; OpenPolicy; and American Public Power Association, Edison Electric Institute, Electric Power Supply Association, the Large Public Power Council, and the National Rural Electric Cooperative Association (collectively, Trade Associations). The discussion below addresses the proposals in the NOPR as well as the NOPR comments.

---

[35] NOPR, 188 FERC ¶ 61,175.

[36] *Id.* P 12.

[37] *Id.* P 14.

[38] *Id.*

II. Discussion

18. Pursuant to section 215(d)(2) of the FPA, we approve proposed Reliability Standard CIP-015-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest. We find that proposed Reliability Standard CIP-015-1 improves the cybersecurity posture of the Bulk-Power System by requiring applicable entities to implement INSM to ensure the detection of anomalous network activity indicative of an attack in progress. The proposed Reliability Standard in main addresses the Commission's directives in Order No. 887 and implements INSM by mandating the collection, detection, evaluation of, and appropriate response to anomalous activity for east-west network traffic.[39]

19. While we approve proposed Reliability Standard CIP-015-1, we also determine that the Standard does not fully address the scope of INSM implementation as contemplated in Order No. 887. As discussed below, a reliability and security gap remains because the Standard does not require implementation of INSM for the entire CIP-networked environment, i.e., outside the electronic security perimeter inclusive of EACMS and PACS. To address this gap, we direct NERC, pursuant to section 215(d)(5) of the FPA, to develop and file within 12 months of the effective date of this final rule modifications to Reliability Standard CIP-015-1 to extend INSM implementation to EACMS and PACS outside of the electronic security perimeter.

[39] *See* P 11 *supra*; Order No. 887, 182 FERC ¶ 61,021 at PP 79-80.

20. Below, we discuss the following: (A) proposed Reliability Standard CIP-015-1; (B) extending INSM to EACMS and PACS beyond the electronic security perimeter; and (C) the timeline to develop modifications to proposed Reliability Standard CIP-015-1.

A. Proposed Reliability Standard CIP-015-1

1. NOPR

21. In the NOPR, the Commission proposed to approve proposed Reliability Standard CIP-015-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

2. Comments

22. NERC, NESCOE, OpenPolicy, and Trade Associations support the Commission's proposal to approve proposed Reliability Standard CIP-015-1.[40] NERC, OpenPolicy, and Trade Associations indicate that proposed Reliability Standard CIP-015-1 would improve the detection of anomalous, malicious, or unauthorized network activity.[41] NERC and OpenPolicy both note that improved detection of anomalous or malicious activity will strengthen responses to and recovery from threats and attacks.[42] No commenters oppose approval of the proposed Reliability Standard.

23. NERC asserts that proposed Reliability Standard CIP-015-1 would strengthen the reliability of the Bulk-Power System by requiring INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity

---

[40] NERC Comments at 2; NESCOE Comments at 3; OpenPolicy Comments at 1; Trade Associations Comments at 2.

[41] NERC Comments at 2; OpenPolicy Comments at 3; Trade Associations Comments at 2.

[42] NERC Comments at 2; OpenPolicy Comments at 2.

inside an electronic security perimeter.[43] According to NERC, the proposed Standard would further improve the cybersecurity posture of the Bulk-Power System by providing visibility into east-west communications within the electronic security perimeter.[44]

24. NESCOE recommends that the Commission "take all necessary steps" to protect the security of the electric grid from malicious actors as new technologies with cybersecurity vulnerabilities are integrated into the grid.[45] Thus, NESCOE states that it supports the NOPR proposals, noting that the proposals are aimed at closing a reliability and security gap.

25. OpenPolicy, while supporting approval of proposed Reliability Standard CIP-015-1, also recommends ways to strengthen the proposed Standard. For example, OpenPolicy proposes adopting scalable and modular INSM architectures to adapt to evolving cybersecurity threats by enhancing threat detection and simplifying compliance processes; and mandating robust encryption standards to secure logs against tampering and unauthorized access.[46]

3. Commission Determination

26. Pursuant to section 215(d)(2) of the FPA, we adopt the NOPR proposal to approve proposed Reliability Standard CIP-015-1 as just, reasonable, not unduly discriminatory or preferential, and in the public interest.

---

[43] NERC Comments at 2.

[44] *Id.* at 3.

[45] NESCOE Comments at 2-3.

[46] OpenPolicy Comments at 2-4.

27. We agree with NERC, OpenPolicy, and Trade Associations that proposed Reliability Standard CIP-015-1 will improve detection of anomalous, malicious, or unauthorized network activity, assisting responsible entities in responding to cyber attacks within the electronic security perimeter.[47] We determine that improved detection and response to cyber attacks and visibility into east-west communication—lacking in other CIP Reliability Standards—will improve the security posture of the electric industry, strengthening the reliability of the Bulk-Power System.[48] Further, we find that proposed Reliability Standard CIP-015-1 fulfills the directive in Order No. 887 to require responsible entities to implement INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity, albeit only within the electronic security perimeter. Additionally, proposed Reliability Standard CIP-015-1 satisfies the directive in Order No. 887 that the Reliability Standard address the three security objectives for east-west network traffic.

28. We decline to direct NERC to modify the proposed Standard to address OpenPolicy's recommendations. We note, however, that responsible entities, in addition to implementing the INSM requirements set forth in proposed Reliability Standard CIP-015-1, may voluntarily choose to adopt additional INSM practices such as those recommended by OpenPolicy. Moreover, OpenPolicy or other entities may advocate for OpenPolicy's recommendations in the NERC Reliability Standard development process.

---

[47] NERC Comments at 2; OpenPolicy Comments at 3; Trade Associations Comments at 2.

[48] NERC Comments at 2; OpenPolicy Comments at 4. *See supra* note 22, explaining east-west communication.

B. Extending INSM to EACMS and PACs Beyond the Electronic Security Perimeter

1. NOPR

29. In the NOPR, the Commission described as overly narrow NERC's proposed application of the term CIP-networked environment because it was limited to assets and systems within the electronic security perimeter. The Commission explained that "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 target of attacks."[49]

30. In the NOPR, the Commission explained that 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.[50] The Commission explained that excluding certain grouped systems from protections—as is the case for EACMS and PACS in proposed Reliability Standard CIP-015-1—leaves other grouped systems within the CIP-networked environment at risk.[51] A compromised

---

[49] NOPR, 188 FERC ¶ 61,175 at P 15.

[50] *Id.* P 16 (citing 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)).

[51] *Id*.

EACMS grouping could provide an attacker with the ability to infiltrate other connected groups, such as BES Cyber Systems located within the electronic security perimeter, as an authenticated user or trusted communication.[52]

31. The NOPR stated that attacks that threaten reliability can emanate from outside the electronic security perimeter from connected Cyber Assets, such as EACMS.[53] 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.[54]

2. Comments

a. Requests to Clarify the Scope of the Term CIP-Networked Environment

32. IRC, NERC, and Trade Associations request that the Commission provide greater clarity about the scope and reach of the term CIP-networked environment.[55] NERC and Trade Associations assert that the term is ambiguous and not defined.[56]

---

[52] *Id.*

[53] *Id.* P 18 (citing CISA, *Cybersecurity Advisory: CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks*, 1, 2 (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 (CISA Cybersecurity Advisory).

[54] *Id.* P 19. The National Institute of Standards and Technology (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, *NIST SP 800-215 Guide to a Secure Enterprise Network Landscape*, 5 (Nov. 2022), https://doi.org/10.6028/NIST.SP.800-215 (NIST SP 800-215).

[55] IRC Comments at 2; NERC Comments at 3; Trade Associations Comments at 8.

[56] NERC Comments at 3-4; Trade Associations Comments at 8, 12.

33. NERC asks two clarifying questions. First, NERC asks whether, in extending the INSM protections to EACMS and PACS, would the term CIP-networked environment be restricted to east-west communications between EACMS and PACS outside of the electronic security perimeter.[57] Second, NERC asks whether the term should include the communications between PACS and controllers and communications to and from EACMS used solely for electronic access monitoring.[58]

34. IRC recommends that the Commission clarify the term by specifying in a final rule "the networks located outside of a responsible entity's Electronic Security Perimeter" that would be subject to INSM requirements.[59]

35. OpenPolicy supports a broad definition of the term CIP-networked environment. It believes that the term must include information technology, operational technology, and internet of things systems and all converged assets to achieve the full potential of extending INSM implementation beyond the electronic security perimeter.[60] OpenPolicy claims this expansive definition of the term will mitigate risks associated with lateral movement and blind spots, providing comprehensive network security.[61] Additionally, OpenPolicy asserts that incorporating operational technology systems into INSM frameworks is needed for segmenting and monitoring operational technology traffic to

---

[57] NERC Comments at 5-6.

[58] *Id.* at 6.

[59] IRC Comments at 2.

[60] OpenPolicy Comments at 2.

[61] *Id.*

prevent lateral movement in industrial automation and control environments that can cause significant operation disruptions.[62]

b. Directive to Extend INSM Implementation to EACMS and PACS Beyond the Electronic Security Perimeter

36. NERC, NESCOE, and OpenPolicy support the proposed directive to extend INSM implementation to EACMS and PACS outside of the electronic security perimeter.[63] NERC comments that it agrees with the Commission "that additional reliability benefits may be achieved by extending INSM implementation to EACMS and PACS beyond the electronic security perimeter."[64]

37. Likewise, NESCOE supports the proposed directive to extend the scope of INSM implementation, because the directive is aimed at closing a reliability and security gap that malicious actors could exploit to target the electric grid.[65] NESCOE explains that attackers could use network and supply chain attacks to bypass network perimeter-based security controls.[66]

38. OpenPolicy states that the proposed "directive to extend INSM requirements beyond traditional electronic security perimeters is a commendable step forward."[67] OpenPolicy explains that monitoring east-west traffic within trust zones enables the early

---

[62] *Id.* at 3.

[63] NERC Comments at 3; NESCOE Comments at 3; OpenPolicy Comments at 2.

[64] NERC Comments at 3.

[65] NESCOE Comments at 3.

[66] *Id.* at 3 n.10 (citing Order No. 887, 182 FERC ¶ 61,021 at P 15).

[67] OpenPolicy Comments at 2.

detection of unauthorized activity that bypass traditional perimeter defenses, enhancing both incident response and risk management by providing a holistic view of potential vulnerabilities.[68] Further, OpenPolicy notes that EACMS and PACS are critical for operational control and that extending INSM implementation to EACMS and PACS addresses attacks that originate from connected cyber assets outside traditional trust zones.[69]

39. Trade Associations oppose the Commission's proposal to direct NERC to modify proposed Reliability Standard CIP-015-1 to expand the scope of INSM to include EACMS and PACS outside of the electronic security perimeter.[70] Trade Associations assert that INSM implementation should focus on the "most critical environment" (i.e., networks protected by the electronic security perimeter) and should not be extended to EACMS and PACS.[71] According to Trade Associations, the industry would face budget, supply chain, and workforce constraints in extending INSM implementation to EACMS and PACS outside the electronic security perimeter.[72] Trade Associations continue that industry may need to employ multiple tools to implement INSM inside and outside the electronic security perimeter due to differences in the operating environments, resulting

---

[68] *Id.*

[69] *Id.* at 2-3.

[70] Trade Associations Comments at 2, 6.

[71] *Id.* at 6.

[72] *Id.* at 6-7.

in an increased volume of network traffic and false positives for events and causing alert fatigue.[73]

40. Trade Associations further argue that, should the Commission require application of INSM to external EACMS and PACS, the Commission should allow the NERC standard drafting team flexibility to "focus on EACMS and PACS that have the greatest impact on grid security."[74] Trade Associations assert that "not all EACMS and PACS are high risk" and continue that revisions to CIP Reliability Standards should be "risk based and outcome oriented."[75] According to Trade Associations, EACMS and PACS that perform (or rely on) access control functions pose a higher risk, while those that perform a monitoring function such as a security information and event management solution presents a lower reliability risk. Consequently, Trade Associations aver that any revisions to the scope of proposed Reliability Standard CIP-015-1 account for "variations in the criticality and risk of these assets in order for it to be a risk-based Standard focused on protecting the most critical, high-risk assets that, for reliability, pose the greatest risk to the BES."[76]

41. Trade Associations also suggest that instead of directing NERC to extend INSM implementation at this time, the Commission should direct NERC to conduct a feasibility study after the Standard's implementation to review intelligence reports about malicious activity targeting EACMS and PACS that may have a material impact on the reliability of

---

[73] *Id.* at 7.

[74] *Id.* at 8.

[75] *Id.*

[76] *Id.*

the Bulk-Power System.[77] The feasibility study would help the Commission determine if there is residual risk to be addressed in other environments.[78] Finally, Trade Associations request that, if the Commission directs NERC to extend INSM implementation to EACMS and PACS outside the electronic security perimeter, the Commission support NERC in establishing a noncompliance abeyance period in light of complexities and resource constraints associated with implementation of INSM.[79]

42. IRC requests that the Commission should direct NERC to extend INSM implementation "*to networks on which* [EACMS] and [PACS] reside outside of a responsible entity's Electronic Security Perimeter."[80] IRC asks the Commission to clarify that the proposed directive to require INSM for EACMS and PACS external to the electronic security perimeter does not require "changes to the CIP-015-1 approach of directing responsible entities to use a risk-based rationale to implement network activity monitoring inside or outside an Electronic Security Perimeter."[81]

3. Commission Determination

a. Scope of the Term CIP-Networked Environment

43. We are persuaded by the comments of NERC, IRC, and Trade Associations to clarify the scope of the term CIP-networked environment. First, the term CIP-networked environment does not cover all of a responsible entity's network. Rather, the scope of

---

[77] *Id.* at 6, 8.

[78] *Id.* at 8.

[79] *Id.* at 12.

[80] IRC Comments at 2.

[81] *Id.*

CIP-networked environment includes the systems within the electronic security perimeter *and* one or more of the following: (1) network segments that are connected to EACMS and PACS outside of the electronic security perimeter; (2) network segments between EACMS and PACS outside of the electronic security perimeter; or (3) network segments that are internal to EACMS and PACS outside of the electronic security perimeter.[82] We determine that the above scope is appropriate because compromised EACMS and PACS outside the electronic security perimeter can provide an avenue for an attacker to access the operational technology environment inside the electronic security perimeter[83] to undertake any number of malicious acts as described in Order No. 887.[84] Implementation of INSM at each of the above networked segments should allow a responsible entity to detect and respond to malicious or unauthorized access to the electronic security perimeter. The below graphic depicts the CIP-networked environment (i.e., the "trust zone") that consists of the Cyber Systems, including the delineated networked segments mentioned in this paragraph (documented in arrows), that are subject to the INSM

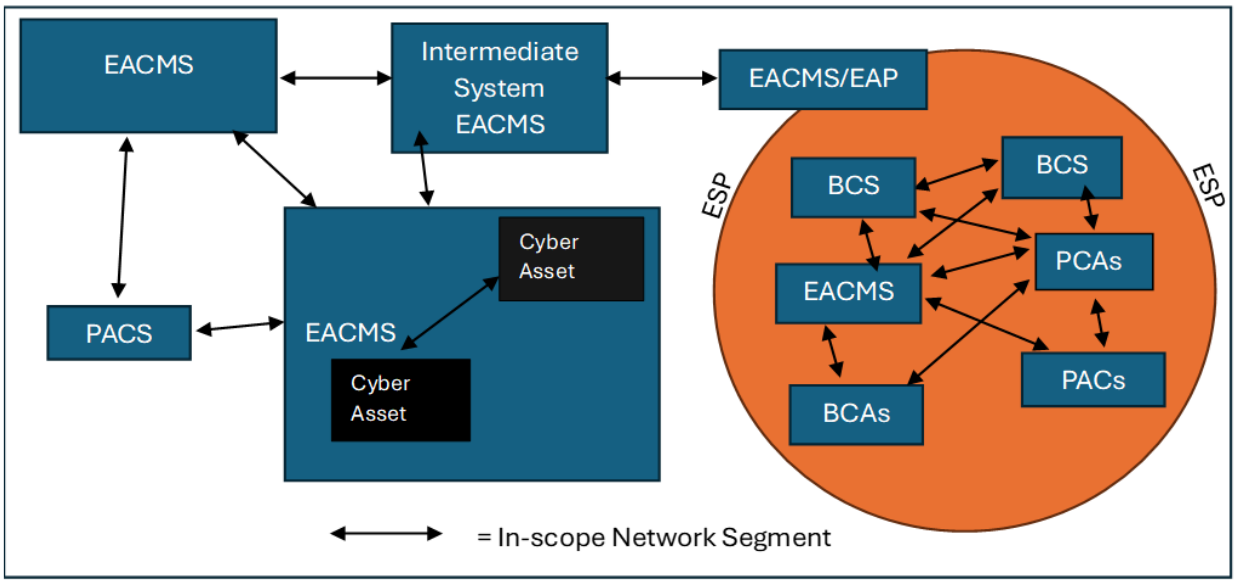
---

[82] To clarify, the CIP-networked environment is comprised of all high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity that are subject to CIP Reliability Standards and may be targets of attacks. *See* NOPR, 188 FERC ¶ 61,175 at P 15.

[83] *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 a compromised domain controller, typically located at an EACMS).

[84] Order No. 887, 182 FERC ¶ 61,021 at P 19 ("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).").

requirements of this final rule.



44. The term CIP-networked environment is inclusive of EACMS and PACS necessary to protect all trust zones of the term[85] and extends beyond the electronic security perimeter to guard against attackers moving east-west within the EACMS or PACS network segments of the term.[86]

45. Consistent with the additional clarity about the scope of the term CIP-networked environment provided above, we answer NERC's questions. First, in extending proposed Reliability Standard CIP-015-1 to EACMS and PACS, CIP-networked environment encompasses east-west traffic within EACMS networks and PACS networks, as well as east-west traffic between EACMS and PACS, in addition to east-west traffic within the electronic security perimeter. Second, communication between PACS and controllers and communications to and from EACMS used solely for electronic access monitoring are included in the term CIP-networked environment.

---

[85] *Id.* P 14.

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

46. We note that one aspect of OpenPolicy's recommended definition of the term CIP-networked environment is already incorporated into the delineated network segments discussed above: implementation of INSM at operational technology environments,[87] guarding against disruptions in industrial and control environments.[88] OpenPolicy's proposal to extend the definition of the term CIP-networked environment to include information technology and internet of things environments[89] is outside the scope of this proceeding, which focuses on INSM implementation in operational technology environments.

b. Directive to Extend INSM to EACMS and PACS Outside the Electronic Security Perimeter

47. Pursuant to section 215(d)(5) of the FPA, we adopt the NOPR proposal to direct NERC to develop modifications to proposed Reliability Standard CIP-015-1 to extend INSM implementation to EACMS and PACS outside of the electronic security perimeter. We find that proposed Reliability Standard CIP-015-1 is not fully responsive to the directive in Order No. 887 to implement INSM within the CIP-networked environment

---

[87] OpenPolicy Comments at 2. The NIST Glossary defines operational technology to mean "[p]rogrammable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms." NIST, *Computer Security Resource Center, Glossary* (Mar. 10, 2022), https://csrc.nist.gov/glossary.

[88] *See* NIST, *NIST SP 800-82r3 Guide to Operational Technology (OT) Security*, 1, 12 (Sept. 2023), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (describing operational technology security as vital to the operation of critical U.S. infrastructure, including electrical utility transmission and distribution systems) (NIST SP 800-82r3).

[89] OpenPolicy Comments at 2.

because proposed Reliability Standard CIP-015-1 excludes EACMS and PACS, which leaves a security gap.

48. We agree with commenters that extending INSM implementation to EACMS and PACS outside the electronic security perimeter provides reliability benefits by closing a reliability and security gap through addressing potential attack vectors that originate outside the trust zone.[90] Extending INSM implementation ensures that BES Cyber Systems benefit from monitoring of east-west traffic within groups of EACMS and PACS.[91] The inclusion of EACMS and PACS enhances early detection of anomalous or malicious activity. Accordingly, our directive fills a reliability gap by addressing potential avenues for attackers to infiltrate BES Cyber Systems within the electronic security perimeter.[92]

49. We are unpersuaded by Trade Associations' arguments for opposing the extension of INSM implementation to EACMS and PACS outside of the electronic security perimeter. The "most critical environment" is broader than envisioned by Trade

---

[90] NERC Comments at 3; NESCOE Comments at 3; OpenPolicy Comments at 2.

[91] *See* CISA Cybersecurity Advisory at 2, 14 (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 identity and access management system, e.g., Active Directory serving as an electronic access control system); NIST SP 800-215 at 5 (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 800-82r3 at 74 (recommending the analyzing of information to differentiate between known and unknown communication as a necessary first step in implementing network security monitoring). The term INSM is used by the Commission in Order No. 887, but the cybersecurity industry uses the term "network security monitoring."

[92] *See* CISA Cybersecurity Advisory at 2-6 (describing how a CISA Red Team gained access to workstations and servers from an identity and access management system serving as an electronic access control system, which assisted in lateral movement to other networks).

Associations. As a NIST guidance document explains, INSM improves the probability of detection for anomalous or malicious activity and should not be isolated to the most critical trust zone (i.e., the electronic security perimeter).[93] Otherwise, a threat already in the most critical trust zone can move laterally within the network and remain undetected for an extended period of time.[94] A threat that can move laterally within the network can threaten the reliability of the Bulk-Power System.[95]

50. In fine, "access controls" in the EACMS acronym refer to user passwords and other information that, once compromised, enables an adversary to enter and move undetected within a network.[96] These are known targets for malicious actors.[97] The risk is similar regardless of whether EACMS and PACS reside inside or external to the electronic security perimeter.

51. Likewise, we disagree with Trade Associations' assertion that meaningful distinctions can be made within categories of EACMS and PACS based on level of risk.

---

[93] *See* NIST SP 800-215 at 5 (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").

[94] *Id.*

[95] *See* CISA Cybersecurity Advisory at 2, 14 (a CISA red team avoided detection and gained access to an organization's network through lateral movement by leveraging access to an identity and access management system serving as an electronic access control system).

[96] For example, virtual private network (VPN) connections fit the definition of EACMS.

[97] *See* AUS GOV'T ET AL., *Detecting and Mitigating Active Directory Compromises* ii (Jan. 2025), https://www.cyber.gov.au/sites/default/files/2024-09/PROTECT-Detecting-and-Mitigating-Active-Directory-Compromises.pdf (explaining that one such EACMS "is susceptible to compromise due to its permissive default settings, its complex relationships, and permissions…. These issues are commonly exploited by malicious actors to compromise" the system).

Trade Associations acknowledge what they characterize as the higher risk associated with EACMS and PACS that perform access control functions but suggest that those performing monitoring functions pose a lesser risk. This distinction is unfounded.[98] EACMS and PACS that perform monitoring functions also are susceptible to a level of risk that warrant INSM. For example, a compromised monitoring system such as the security information and event management referenced by Trade Associations at minimum gives a malicious actor visibility to information used to control network access. Such reconnaissance can be used by an actor to pre-position for a cyber attack.[99] In other words, an adversary that has gained access to a monitoring system can then obtain the information needed to establish a trusted connection and compromise the electronic security perimeter. Thus, while one or more additional steps may be involved, the risk of network compromise remains high once an adversary gains access to a monitoring system. Regardless of the function of the EACMS, it can serve as a gateway for a malicious actor to compromise the electronic security perimeter and therefore the EACMS warrants protection through INSM implementation.

---

[98] Further, we note that the NERC Glossary definition of EACMS explicitly includes both electronic access controls and electronic access monitoring. *See* NERC Glossary (defining EACMS as "Cyber Assets that perform electronic access control or electronic access *monitoring* of the Electronic Security Perimeter(s) or BES Cyber Systems…" (emphasis added)). We are concerned that Trade Associations' suggestion to distinguish among categories of EACMS would effectively modify the NERC Glossary definition of EACMS.

[99] *See* CISA, *Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* 6, 9 (Feb. 2024), https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf (describing how Volt Typhoon actors conducted extensive pre-compromise reconnaissance to learn about the target organization, its network, and its staff in advance of a possible cyber attack) (PRC State-Sponsored Actors Joint Cybersecurity Advisory).

52. We recognize that NERC in modifying the Standard in response to the directive in this final rule retains the ability to propose an equally efficient and effective solution to determining which EACMS and PACS outside of the electronic security perimeter should be covered by the Standard. However, we caution that Trade Associations' approach appears to fall short of that criteria as it would leave a reliability gap that malicious actors could exploit by using EACMS and PACS outside the electronic security perimeter to penetrate the electronic security perimeter. The additional clarity provided in this final rule should be sufficient for the drafting team to develop a Reliability Standard that is fully responsive to the directive in Order No. 887 to implement INSM within the CIP-networked environment.

53. We are unpersuaded by the Trade Associations' contention that if INSM implementation is not limited to EACMS and PACS that "most disproportionally affect the grid," it could lead to "costly and inefficient deployments and increased traffic" as EACMS and PACS do not share the same requirements as operating technology protocols.[100] Trade Associations provide no evidence for this claim. We believe that the benefits of implementing INSM at the network segments listed above will outweigh the costs of doing so because they are high value targets that if compromised would allow an attacker to infiltrate the perimeter as a trusted communication.[101] Further, responsible entities can take certain steps to mitigate the cost impacts of extending INSM to EACMS and PACS outside the electronic security perimeter by implementing INSM in a risk-

---

[100] Trade Associations Comments at 9.

[101] *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); NIST SP 800-215 at 5; NSA Network Security Guide at 2.

based manner pursuant to Requirement R1.1 of proposed Reliability Standard CIP-015-1. For example, a responsible entity could define incident alert thresholds and establish a baseline for normal network activity that could reduce the cost of retaining and protecting INSM data under Requirements R2 and R3, respectively, by reducing the amount of INSM data responsible entities must collect.[102]

54. Similarly, in response to the Trade Associations' claim that INSM implementation outside of the electronic security perimeter may require the use of multiple tools that could result in increased traffic and false positives that cause alert fatigue,[103] we remind responsible entities that they will determine how to implement INSM based on their architecture and tools (subject to oversight by the compliance enforcement authority), even if revised Reliability Standard CIP-015-1 mandates which cyber assets are subject to INSM requirements. Again, that could mean setting incident alert thresholds and creating baselines for network activity that alert responsible entities only of network traffic that has indicia of malicious intent, reducing the potential for false positive and alert fatigue.

55. Regarding whether to support NERC's potential future establishment of a noncompliance abeyance,[104] we decline to prejudge the need for such a period. We also decline to direct NERC to conduct a feasibility study that includes a review of threat

---

[102] As requested by IRC, we affirm that the directive in this final rule requires no changes to proposed Reliability Standard CIP-015-1 Requirement R1.1 regarding use of a risk-based approach to implement network activity monitoring.

[103] Trade Associations Comments at 7.

[104] *N. Am. Elec. Reliability Corp.*, 189 FERC ¶ 61,211 (2024) (approving NERC's 2024 five-year performance assessment); N. Am. Elec. Reliability Corp., Supplemental Filing, Docket No. RR24-4-000, at 12 (filed Nov. 8, 2024) ("During the standards development process of new and modified Reliability Standards, the ERO Enterprise will consider whether draft Reliability Standards are good candidates for a Potential Noncompliance abeyance period.").

intelligence information containing indicia of malicious activity targeting EACMS or PACS that may have a material impact on the reliability of the Bulk-Power System.[105] This threat is already well-established, and a feasibility study is unnecessary. For example, open-source intelligence reports indicate that malicious actors are targeting an identity and access management system, serving as an electronic access control system, to enable lateral movement—the type of movement INSM is intended to detect and respond to—to gain access to critical operational technology trust zones that can disrupt electrical substations, impacting Bulk-Power System reliability.[106] Similarly, a 2024 CISA cybersecurity alert warned that threat actors were actively exploiting vulnerabilities in certain VPNs that are a type of EACMS used in the electric industry.[107] In addition, NERC's 2024 Annual Report on Cyber Security Incidents noted that two of the three cybersecurity incidents in the report involving the Bulk-Power System were attempts to compromise EACMS outside of the electronic security perimeter.[108] These reports

---

[105] Trade Associations Comments at 8.

[106] *See* PRC State-Sponsored Actors Joint Cybersecurity Advisory at 6-7, 14 (describing how Volt Typhoon attacks achieved full domain compromise by extracting an identity and access management system database that enables potential disruptions, such as disrupting electrical substations).

[107] CISA, *Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms* (Apr. 2024), https://www.cisa.gov/news-events/alerts/2024/04/24/cisco-releases-security-updates-addressing-arcanedoor-vulnerabilities-cisco-firewall-platforms; NERC Glossary. VPNs are commonly used in the electrical industry and if successfully targeted can cause significant operational disruptions in the industry. DRAGOS, *Why Adversaries Target VPN Appliances: The Pathway from IT to OT Cyber Attack*, (Sept. 30, 2024) https://www.dragos.com/blog/why-adversaries-target-vpn-appliances-the-pathway-from-it-to-ot-cyber-attack/.

[108] N. Am. Elec. Reliability Corp., Annual Report of the North American Electric Reliability Corporation on Cyber Security Incidents, Docket No. RM18-2-000 (filed Mar. 21, 2025).

demonstrate that the threat to EACMS and PACS outside of the electronic security perimeter is well-documented and illustrate the residual risk to be addressed in environments outside of the electronic security perimeter.

56. We decline IRC's request to specify the networks located outside of the electronic security perimeter that would be covered by the directed modifications to proposed Reliability Standard CIP-015-1. Such a step is unnecessary following our clarification above regarding the term CIP-networked environment.

C. The Implementation Timeline to Develop Modifications to CIP-015-1

1. NOPR

57. In the NOPR, the Commission proposed to direct NERC to submit the revised Reliability Standard CIP-015-1 extending INSM implementation to EACMS and PACS outside the electronic security perimeter for Commission approval within 12 months of the effective date of a final rule in this proceeding.[109]

2. Comments

58. NERC asks the Commission to provide at least 12 months to modify Reliability Standard CIP-015-1, explaining that it is addressing multiple high priority projects as part of its large workload on Commission directives.[110] NERC notes that providing more than 12 months for implementation of the final rule would allow for additional development options, including a technical conference near the beginning of the development process

[109] NOPR, 188 FERC ¶ 61,175 at P 21.

[110] NERC Comments at 6-7 (as of November 2024, NERC is working on responding to 82 outstanding Commission directives through the Standards Development process).

to promote efficient development and drafting.[111] Additionally, more than 12 months would allow NERC to balance resources between competing high priority projects.

59. Trade Associations express concern that a drafting team may not be able to deliver a Standard within 12 months and ask that the Commission grant NERC the discretion to determine when to submit to the Commission the modification to Reliability Standard CIP-015-1.[112] Further, Trade Associations explain that implementation of the final rule should be extended because the scope of the directed modification may be impacted by Project 2023-09 Risk Management for Third-Party Cloud Services' possible revision of the definition of EACMS.[113] Trade Associations claim that revisions to the definition of EACMS would have significant implications for the scope of modifications to Reliability Standard CIP-015-1. Trade Associations also argue that a timeline extension is necessary as the expansion in the scope of the Standard may not be as simple as "adding additional applicability to the drafted requirements" of Reliability Standard CIP-015-1.[114] Finally, Trade Associations request that the Commission consider organizing a technical workshop or conference as part of the project timeline to define the scope and technical justification of the directed modification to Reliability Standard CIP-015-1.[115]

---

[111] *Id.* at 7-8.

[112] Trade Associations Comments at 10-11.

[113] *Id.* at 12.

[114] *Id.*

[115] *Id.*

3. Commission Determination

60. Based on our consideration of the record, we adopt the 12-month deadline proposed in the NOPR. While we recognize that parties might benefit from additional time, we are not persuaded at this time that additional time is needed to address the modifications directed in this order. To the extent NERC concludes during the standards drafting process that additional time is needed, NERC may request, and the Commission will consider whether to grant, an extension at that time.

III. Information Collection Statement

61. 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 collections of information unless the collections of information display a valid OMB control number. The Commission received no comments on the validity of the burden and cost estimates in the NOPR.

62. 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.

63. 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. Reliability Standard CIP-015-1 does not require applicable entities to submit any filings with either the Commission or NERC as the ERO. Entities, however, are required to maintain documentation adequate to demonstrate compliance with the Reliability Standard. Commission and NERC staff conduct periodic audits of entities and auditors rely on the entity's documentation in determining compliance with a Reliability Standard. While entities retain flexibility on how they choose to demonstrate compliance, the Reliability Standard includes Compliance Measures providing examples of the type of documentation an entity may want to develop and maintain to demonstrate compliance. The reporting burden below is based on the Compliance Measurements provided in Reliability Standard CIP-015-1.

64. The NERC Compliance Registry, as of April 2025, 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 in the Final Rule in Docket No. RM24-7-000[116]						
	Number of Respondents (1)	**Annual Number of Responses per Respondent (2)**	**Total Number of Responses (1)*(2)=(3)**	**Average Burden & Cost Per Response[117] (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.; $3,410	16,000 hrs.; $1,364,160	$3,410
Create documentation detailing network data feed(s) and reason (R1.1)	400	1	400	60 hrs.; $5116	24,000 hrs.; $2,046,240	$5,116
Create documentation of: anomalous events and baseline used to detect anomalous events (R1.2)	400	1	400	60 hrs.; $5,116	24,000 hrs.; $2,046,240	$5,116
Create documentation of methods to: evaluate anomalous activity; response to detected activity; and escalation process(es) (R1.3)	400	1	400	60 hrs.; $5,116	24,000 hrs.; $2,046,240	$5,116

[116] The paperwork burden estimate includes costs associated with the initial development of a policy to address the requirements.

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

The loaded hourly wage figure (includes benefits) is based on the average of three occupational categories for May 2024 Wages found on the Bureau of Labor Statistics website (http://www.bls.gov/oes/current/naics2_22.htm). The loaded hourly wage includes fringe benefits divided by 81.70%. *See* https://data.bls.gov/oes/#/industry/000000:

Legal Occupations (90th percentile) (Occupation Code: 23-0000): $140.76

Electrical Engineer (mean) (Occupation Code: 17-2071): $71.19

Office and Administrative Support (90th percentile) (Occupation Code: 43-0000): $43.83

($140.76 + $71.19 + $43.83) ÷ 3 = $85.26

The figure is rounded to $85.00 for use in calculating wage figures in this final rule.

Create documentation of: data retention process(es); system configuration(s), or system-generated report(s) (R2)	400	1	400	60 hrs.; $5,116	24,000 hrs.; $2,046,240	$5,116
Create documentation of how the collected data is being protected (R3)	400	1	400	60 hrs.; $5,116	24,000 hrs.; $2,046,240	$5,116
Total burden for FERC-725B(5) under CIP-015-1			2,400		136,000 hrs.; $11,595,360	$32,116

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

- Year 1-3 each: 2,400 responses; 136,000 hours

66. The annual cost burden for each year One to Three is $11,595,360.

67. 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 final rule approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves 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.

68. 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].

IV. Environmental Analysis

69. 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.[118] 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.[119] The action proposed herein falls within this categorical exclusion in the Commission's regulations.

---

[118] *Reguls. Implementing the Nat'l Env't 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).

[119] 18 CFR 380.4(a)(2)(ii).

V. Regulatory Flexibility Act

70. The Regulatory Flexibility Act of 1980 (RFA)[120] generally requires a description and analysis of final 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.[121] 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).[122] The Commission believes that because the obligations imposed upon industry are directed only at 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, only a minimal number of entities will meet the SBA revised standard for electric utilities. Only a minimal number of entities will satisfy the SBA revised standard because small entities do not typically own or operate any kind of high impact BES Cyber Systems or medium impact BES Cyber systems with external routable connectivity. Therefore, the Commission certifies that this final rule will not have a significant economic impact on a substantial number of small entities. Accordingly, no regulatory flexibility analysis is required.

VI. Document Availability

71. 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

---

[120] 5 U.S.C. 601-612.

[121] 13 CFR 121.101.

[122] 13 CFR 121.201, Subsector 221 (Utilities).

contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov).

72. 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.

73. 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 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.

VII. Effective Date and Congressional Notification

74. These regulations are effective **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION 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 section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996.

Issued: June 26, 2025.

Carlos D. Clay,

Deputy Secretary.

[FR Doc. 2025-12309 Filed: 7/1/2025 8:45 am; Publication Date: 7/2/2025]