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

COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION, EDISON ELECTRIC INSTITUTE, ELECTRIC POWER SUPPLY ASSOCIATION, LARGE PUBLIC POWER COUNCIL, AND NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

The American Public Power Association (APPA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), the Large Public Power Council (LPPC), and the National Rural Electric Cooperative Association (NRECA) (together, the Trade Associations) respectfully submit the following comments in response to the Notice of Proposed Rulemaking (NOPR) issued in this docket by the Federal Energy Regulatory Commission (FERC or Commission) on September 19, 2024.[1] For the reasons provided in these comments, the Trade Associations respectfully ask the Commission to adopt in its final rule the recommendations put forth herein.

The NOPR proposes to approve CIP Reliability Standard CIP-015-1 (Cyber Security – Internal Network Security Monitoring), as approved by the North American Electric Reliability Corporation (NERC), and further proposes to direct NERC to modify this proposed Standard to extend internal network security monitoring (INSM) to include Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) outside of the

[1] *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring*, Notice of Proposed Rulemaking, 188 FERC ¶ 61,175 (2024).

Electronic Security Perimeter (ESP).[2] According to FERC, the proposed modification is needed to bring proposed Reliability Standard CIP-015-1 in line with its directive in Order No. 887.[3]

The Trade Associations support the Commission's proposal to approve proposed Reliability Standard CIP-015-1. We agree that there are benefits associated with implementing INSM within the ESP, such as earlier detection and notification of intrusions and malicious activity. Expanding the existing CIP Reliability Standards to include INSM will complement existing network security perimeter monitoring requirements for high- and medium-impact Bulk Electric System (BES) Cyber Systems through improved internal network communications visibility.

However, for the reasons put forward later in these comments, we oppose the Commission's proposal to require NERC to modify proffered Reliability Standard CIP-015-1 to expand the scope of INSM outside of the ESP to EACMS and PACS.

I. IDENTIFICATION OF FILING PARTIES

APPA is the national service organization representing the interests of not-for-profit, state, municipal, and other locally owned electric utilities in the United States. More than 2,000 public power systems provide over 15% of all kilowatt-hours sales to ultimate customers in the United States and serve over 49 million people, doing business in every state except Hawaii. Over 240 public power utilities are registered entities subject to compliance with mandatory NERC Reliability Standards.

EEI is the association that represents all U.S. investor-owned electric companies. EEI members provide electricity to more than 250 million Americans and operate in all 50 states and the District of Columbia. The electric power industry supports more than seven million jobs in

[2] *Id.* ¶ 1.
[3] *Id.* ¶ 3.

communities across the United States. EEI members are investing $170 billion annually to make the energy grid more secure against all hazards, including cybersecurity threats. The EEI member companies' approach to cybersecurity is driven by factors unique to their operational environment—including (but not limited to) their operational safety; regulatory requirements; affordability; and threat-informed, risk-based analysis.

EPSA is the national trade association representing competitive power suppliers in the U.S. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. EPSA seeks to bring the benefits of competition to all power customers. This pleading represents the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

LPPC is an association of 29 of the nation's largest municipal and state-owned utilities, representing the larger, asset-owning members of the public power community and approximately 90% of the transmission assets owned by public power. Located throughout the nation, many of LPPC's members are transmission-owning members of independent system operators (ISOs) and regional transmission organizations (RTOs), while others are considering membership in regions of the nation in which ISOs/RTOs and other organized markets are yet being developed.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are built by and owned by the people that they serve and comprise a unique sector of the electric industry. Electric cooperatives operate at cost and without a profit incentive. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56% of the nation's landmass.

II. BACKGROUND

Order No. 887 directed NERC to develop "new or modified CIP Reliability Standards requiring INSM for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity to ensure the detection of anomalous network activity indicative of an attack in progress."[4] The Commission observed that INSM is "applied within a 'trust zone,' such as an electronic security perimeter" and held that, for the final rule, the applicable trust zone for INSM is the "CIP-networked environment."[5]

As explained by the Commission, Order No. 887's directive was designed to address grid vulnerabilities resulting from cybersecurity risks introduced by actors granted access to the grid. Addressing that perceived reliability gap, FERC ordered NERC to ensure that the new or modified CIP Reliability Standards address the following three security objectives:

> 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 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.

NOPR ¶ 9 (quoting Order No. 887 ¶ 9). Responding to the Commission's directive, NERC developed proposed Reliability Standard CIP-015-1.

---

[4] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 ¶ 3 (2023) (Order No. 887).
[5] *Id.* ¶ 2.

NERC submitted proposed Reliability Standard CIP-015-1 with the Commission for approval on June 24, 2024.[6] According to *NERC's Petition*, proposed Reliability Standard CIP-015-1 satisfies Order No. 887's directives by establishing three requirements. Requirement Rl 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 ESP.[7] Requirement R2 would call for responsible entities to retain INSM data related to anomalous activity.[8] Requirement R3 would compel responsible entities to protect INSM data associated with anomalous network activity.[9]

NERC further states that proposed Reliability Standard CIP-015-1's scope is consistent with the plain language of Order No. 887, which held 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."[10] According to NERC, its approach would provide the greatest benefits to the reliability of the BPS by focusing industry's limited resources on the most critical environment, "networks protected by the Responsible Entity's Electronic Security Perimeter."[11]

On September 19, 2024, the Commission issued the NOPR. In it, FERC proposes to approve recommended Reliability Standard CIP-015-1 and to direct NERC to develop modifications to this Standard that would extend INSM to include EACMS and PACS outside of the ESP, reasoning this revision is needed to address a perceived reliability gap.

---

[6] *See Internal Network Security Monitoring for High & Medium Impact Bulk Electric System Cyber Systems*, Docket No. RM24-7-000, *Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-015-1* (filed June 24, 2024) (*NERC's Petition*).
[7] *Id.* Ex. A (Proposed Reliability Standard CIP-015-1) at 6.
[8] *Id.* at 7.
[9] *Id.*
[10] *NERC's Petition* 13 (quoting Order No. 887 ¶ 2).
[11] *Id.* at 17.

III. COMMENTS

A. The Implementation of INSM Should Focus on the Most Critical Environment, Networks Protected by an ESP, and Should Not Be Extended to EACMS and PACS.

Proposed Reliability Standard CIP-015-1 applies INSM within a trust zone, the ESP, for the most critical resources—high-impact BES Cyber Systems with and without External Routable Connectivity (ERC) and medium-impact BES Cyber Systems with ERC. The Trade Associations agree with NERC's view that the scope and focus of proposed Reliability Standard CIP-015-1 "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.'"[12]

Responding to the NOPR in Docket No. RM22-3-000 preceding Order No. 887, the Trade Associations expressed concern that the tools necessary to implement INSM were at a relatively early stage of development and not widely available. Further, the Trade Associations pointed to a significant shortage in the availability of trained personnel needed to implement INSM programs.[13] NERC underscored these concerns in its *INSM Feasibility Study* filed with the Commission on January 18, 2024, in Docket No. RM22-3-000, as directed in Order No. 887.[14] There, in explaining the challenge posed by the possible extension of an INSM requirement to low-impact BES Cyber Systems and to medium-impact BES Cyber Systems without ERC, NERC points to budget and supply-chain constraints (namely, the ongoing

[12] *NERC's Petition* 16 (quoting Order No. 887 ¶ 2).
[13] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Docket No. RM22-3-000, Comments of the Edison Electric Institute, the American Public Power Association, the Large Public Power Council, the National Rural Electric Cooperative Association, and the Electric Power Supply Association (filed March 28, 2022).
[14] *See Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Docket No. RM22-3-000, *Internal Network Security Monitoring Feasibility Study Report* (filed January 18, 2024) (*INSM Feasibility Study*).

difficulty of sourcing the technology), along with significant limitations on the availability of qualified personnel to install, configure, operate, and maintain monitoring systems; analyze resulting data; and respond to security incidents. While the scope of asset types included in NERC's *INSM Feasibility Study* focused on low-impact BES Cyber Systems and medium-impact BES Cyber Systems without ERC instead of the networks containing EACMS and PACS outside of the ESP, similar concerns about budget, supply chain, and workforce constraints remain.

With the passage of time, the Trade Associations can report a certain amount of progress in connection with the availability of the necessary tools; however, supply-chain bottlenecks and workforce challenges (specifically, difficulties assembling an adequately trained workforce) persist. Moreover, many of the INSM solutions available are designed to be "industrial control system (ICS) protocol aware" and to detect network activity that might hamper an industrial process, making them more valuable for use within an ESP than in the networks where EACMS and PACS reside where the threats are more likely to originate from IT systems.[15] Due to the differences between the environments, deployment of the same INSM system may not be effective, requiring the implementation of multiple tools to achieve INSM requirements. This would result in an increased volume of network traffic and false positives for events that are not relevant to critical infrastructure protection and, in turn, reduce the overall effectiveness of security teams and contribute to alert fatigue.

The Trade Associations respectfully ask the Commission to approve proposed Reliability Standard CIP-015-1 and allow industry to implement INSM within the ESP, enabling

[15] North American Electric Reliability Corporation, *North American Electric Reliability Corporation Technical Rationale for Reliability Standard CIP-015-1* (2024), available at https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023-03%20Technical%20rationale%20document%20Feb2024.pdf.

responsible entities to focus limited resources on assets that, if compromised, could pose the greatest risk to the reliability of the grid. Following the implementation of proposed Reliability Standard CIP-015-1, we ask the Commission to consider directing NERC to conduct another feasibility study with industry that includes a review of threat intelligence information containing indicia of malicious activity targeting EACMS or PACS which may have a material impact on the reliability of the BPS and determine if there is residual risk to be addressed in other environments. NERC could also host a technical conference. This phased approach considers industry constraints, addresses current risks, and provides a mechanism for addressing future identified risks.

B. If the Commission Chooses Not to Limit the Implementation of INSM to Networks Within the ESP, It Should Permit the Drafting Team to Focus on EACMS and PACS That Have the Greatest Impact on Grid Security.

Although the NOPR clarifies that the "CIP-networked environment" was used in Order No. 887 to refer to an environment broader than the ESP and inclusive of EACMS and PACS, it is still not clearly defined. The NOPR does not acknowledge the diversity among implemented network architectures where EACMS and PACS may reside or the diversity of the types of systems classified as EACMS and PACS. The types of systems categorized as EACMS and PACS range from controlling access to monitoring access and represent varying levels of criticality and risk to the BES: not all EACMS and PACS are high risk. However, revisions to NERC CIP Standards should be risk based and outcome oriented. Therefore, any revisions in the scope of proposed Reliability Standard CIP-015-1 must account for the 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 purposes, pose the greatest risk to the BES. In addition, network traffic between an EACMS and an ESP is likely to be captured by an INSM

solution internal to the ESP, while traffic related to PACS and EACMS outside the ESP can be monitored using IT-based systems that many entities have already deployed within their IT environments.

Importantly, the purpose of the INSM is to monitor the flow of data between devices and servers within the ESP, not traffic outside of the ESP. Consequently, as noted in the Trade Associations' NOPR comments submitted in Docket No. RM22-3-000, deploying an INSM system outside of the ESP would be a complex process and present significant technological challenges. Because EACMS and PACS do not share the same requirements as those supporting OT protocols, if the extension of INSM is not limited solely to those EACMS and PACS that most disproportionately affect the grid, expanding the requirement to cover these systems could lead to costly and inefficient deployments and increased traffic within the INSM that would further strain an already limited cyber workforce.

Clarification ensuring that EACMS and PACS included in an expanded Standard are limited to those with significant potential to threaten the grid if compromised should be left to the drafting team. Therefore, we respectfully ask the Commission to expressly provide the drafting team the requisite authority to define the appropriate scope of EACMS and PACS in its final rule. Several of our member companies' subject-matter experts were on the Project 2023-03 drafting team and have stated that, during their deliberations regarding the scope of proposed Reliability Standard CIP-015-1, the drafting team considered the fundamental principles of network security monitoring described in scholarly works, such as Richard Bejtlich's book, *The Practice of Network Security Monitoring*,[16] and Chris Sanders et al.'s work, *Applied Network*

[16] Richard Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response* (1st ed., No Starch Press 2013) (*The Practice of Network Security Monitoring*).

Security Monitoring.[17] These books include information that can also be used by a future drafting team to determine the EACMS and PACS for inclusion in INSM that will provide the most security value, such as those that perform access control functions or those that rely on access control functions. For example, EACMS that are used for authentication provide access control functions that if compromised could have a reliability impact, while a security information and event management (SIEM) solution that is only performing a monitoring function would not pose the same risk to reliability if compromised because it does not have the same ability to allow or deny access to in-scope assets. A scoping approach such as this one reduces the complexity of implementation by reducing the amount of traffic necessary to monitor and takes a risk-based approach by prioritizing assets performing the most critical functions of EACMS and PACS.

C. If the NOPR's Proposal to Modify Proposed Reliability Standard CIP-015-1 Is Adopted in the Final Rule, the NOPR's Compliance Timeline Should Be Altered.

In the event the Commission adopts in its final rule the proposed modification to recommended Reliability Standard CIP-015-1 put forth in this NOPR, the Trade Associations respectfully request that the Commission grant NERC the discretion to determine when to submit the compliance filing, to ensure that the higher-risk issues already approved for development are addressed first.

If the Commission imposes *any* set deadline for completing revisions to Reliability Standard CIP-015-1, we ask for consideration to extend NERC's compliance date for submitting the revised Standard from the proposed 12 months to 12 months following the implementation of CIP-015-1. We also ask that the Commission approve the current version of Reliability Standard

[17] Chris Sanders & Jason Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis* (1st ed. Syngress Publishing 2013).

CIP-015-1 in its final rule to begin the implementation plan period, allowing industry to institute controls meant to reduce risk in the most critical environments.

Due to the large number of high-priority projects already in the queue for completion, the Trade Associations are concerned about the ability to complete the project within 12 months. In 2025, we intend to complete at least seven "high priority" standards projects which NERC anticipates will take more than 10,000 total hours for drafting teams to complete.[18] Moreover, there are 12 additional medium- and low-priority projects in development that are anticipated to continue into 2025.[19] This incredibly fast pace of producing new or modified Reliability Standards is a testament to industry's commitment to address the most significant reliability risks to the BES. Each industry drafting team dedicates hundreds of hours on each project,[20] and hundreds of individual registered entities dedicate substantial time and effort to reviewing and commenting on each revision proposed by the drafting teams. In short: developing high-quality Reliability Standards requires tremendous resources from industry, from NERC staff, and from the Commission. Providing NERC with discretion to determine when to submit the compliance filing affords NERC and industry the flexibility necessary to balance limited resources between competing high-priority projects. The Trade Associations respectfully ask the Commission to consider extending NERC's compliance date for submitting the revised Standard from the proposed 12 months to 12 months following the implementation of Reliability Standard CIP-015-1.

---

[18] *See* North American Electric Reliability Corporation, *North American Electric Reliability Corporation Reliability Standards Development Plan 2025-2027*, at 6 (2024), available at https://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/2025-2027%20%20RSDP_Board.pdf (*2025-2027 RSDP*).

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

[20] *See* North American Electric Reliability Corporation, Docket No. RM05-17-000, *North American Electric Reliability Corporation Informational Filing of Reliability Standards Development Plan 2024–2026*, at A3-A5 (filed December 28, 2023) (describing the anticipated hours for each standard drafting team in 2024).

Further, given the ambiguity in the scoping of the CIP-networked environment and questions related to clarifying the types of EACMS and PACS intended, the drafting team may encounter unanticipated challenges in drafting these revisions. Additionally, the current drafting team for Project 2023-09 Risk Management for Third-Party Cloud Services may revise the definition of an EACMS which has significant implications for the scoping of these revisions. Project 2023-09 is a medium-priority project with a target completion date of the end of 2025.[21] The Trade Associations note that the expansion in scope may not be as simple as adding additional applicability to the drafted requirements in proposed Reliability Standard CIP-015-1 and seek sufficient time to address the revisions. We also respectfully request that the Commission consider convening a technical workshop or conference to help define the appropriate scoping and technical justification as part of the project development timeline.

D. A Potential Noncompliance Abeyance Period for INSM Implementation Would Help to Address Technical, Supply Chain, and Workforce Challenges.

The complexities and resource constraints associated with the implementation of INSM as proposed in Reliability Standard CIP-015-1 will increase with any expansion in scope. Accordingly, the Trade Associations respectfully ask the Commission to consider supporting NERC in establishing a Potential Noncompliance abeyance period during the standards development process to "facilitate productive collaboration with industry to address new or urgent reliability needs in a nimble and agile manner."[22] NERC proposes the use of Potential Noncompliance abeyance periods in its November 8, 2024, *Supplemental Filing* to establish efficiencies in the standards development process by encouraging "entities to share observations

[21] *2025-2027 RSDP* 7.

[22] North American Electric Reliability Corporation, *Supplemental Filing of the North American Electric Reliability Corporation to the Five-Year Electric Reliability Organization Performance Assessment Report in Accordance with 18 C.F.R. § 39.3(c)* 12, Docket No. RR24-4-000 (filed November 8, 2024) (*Supplemental Filing*).

and experiences through implementation of new standards without fear of potential noncompliance (so long as they are acting in good faith) to mitigate reliability risks."[23] Given the technical, supply chain, and workforce challenges described for INSM, an opportunity to implement Reliability Standard CIP-015-1 and any subsequent revisions in good faith would encourage the use of feedback loops to ensure that risks are being addressed as intended.

IV. CONCLUSION

The Trade Associations appreciate the opportunity to submit comments on the proposals provided in this NOPR. The Trade Associations support the Commission's recommendation to approve proposed Reliability Standard CIP-015-1. For the reasons stated herein, the Trade Associations respectfully request that the Commission adopt in its final rule all of the recommendations set forth in these comments.

Respectfully submitted,

/s/ Travis R. Smith, Sr.
Travis R. Smith, Sr.
Associate General Counsel, Reliability and Security
tsmith@eei.org

Andrea Koch
Senior Director, Reliability Policy
akoch@eei.org

Kristine Martz
Director, Reliability Policy
kmartz@eei.org

Edison Electric Institute
701 Pennsylvania Ave., N.W.
Washington, DC 20004
(202) 508-5000

[23] *Id.* at 10.

/s/
Desmarie M. Waterhouse
Senior Vice President of Advocacy and Communications & General Counsel
dwaterhouse@publicpower.org

Latif M. Nurani
Senior Regulatory Counsel
lnurani@publicpower.org

American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

/s/ Mary Ann Ralls
Mary Ann Ralls
Senior Director, Regulatory Affairs
maryann.ralls@nreca.coop

Patricia Metro
Senior Grid Operations & Reliability Director
patti.metro@nreca.coop

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-5837

/s/
Jonathan D. Schneider
STINSON LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com

Counsel to the Large Public Power Council

/s/

Nancy Bagot
Senior Vice President
nbaot@epsa.org

Bill Zuretti
Director, Regulatory Affairs & Counsel
bzuretti@epsa.org

Electric Power Supply Association
1401 New York Avenue, NW, Suite 950
Washington, DC 20005
(202) 628-8200

November 26, 2024

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Commission Secretary in this proceeding in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.2010 (2023).

Dated this 26th day of November 2024 in Washington, D.C.

/s/ Travis R. Smith, Sr.

Travis R. Smith, Sr.
Associate General Counsel, Reliability and Security
202.508.5145

Edison Electric Institute
701 Pennsylvania Ave., N.W.
Washington, DC 20004

Document Content(s)