UNITED STATES OF AMERICA
BEFORE THE
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 NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") submits comments on the Federal Energy Regulatory Commission's ("FERC" or "Commission") Notice of Proposed Rulemaking ("NOPR") regarding Critical Infrastructure Protection Standard CIP-015-1 – Cyber Security – Internal Network Security.[1] Specifically, the Commission seeks comment on its proposals to: (1) approve proposed Reliability Standard CIP-015-1 (Cyber Security – Internal Network Security Monitoring); (2) direct NERC to develop modifications to proposed Reliability Standard CIP-015-1 that would extend internal network security monitoring to include Electronic Access Control or Monitoring Systems ("EACMS") and Physical Access Control Systems ("PACS") outside the Electronic Security Perimeter[2]; and (3) direct NERC to submit the revised Reliability Standard for Commission approval within 12 months of the effective date of a final rule.[3]

As discussed herein, NERC supports FERC's continued efforts to strengthen the cyber security posture of Responsible Entities[4] and to enhance the reliability and security of the Bulk Power System ("BPS"). NERC looks forward to stakeholder comments on the NOPR regarding

---

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

2 *Id.* P 21.

3 *Id.*

4 As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

extending internal network security monitoring to include EACMS and PACS outside the Electronic Security Perimeter in Reliability Standards requirements. NERC provides comments on specific aspects of the Commission's proposal and respectfully requests that the Commission consider these comments in future issuances in this proceeding.

I. COMMENTS

A. NERC supports FERC's proposal to approve proposed Reliability Standard CIP-015-1 to strengthen cybersecurity practices.

NERC strongly encourages the Commission to move forward with its proposal to approve proposed Reliability Standard CIP-015-1 as expeditiously as possible. Proposed Reliability Standard CIP-015-1 is just, reasonable, and not unduly discriminatory and would improve the probability of detecting anomalous or unauthorized network activity in order to facilitate improved response and recovery from an attack. As NERC explains in detail in its petition,[5] proposed Reliability Standard CIP-015-1 would advance the reliability of the BPS by establishing requirements for internal network security monitoring for network traffic inside an Electronic Security Perimeter, and requiring internal network security monitoring for all high impact BES Cyber Systems and medium impact BES Cyber Systems with external routable connectivity to ensure the identification of anomalous network activity. It would accomplish this by establishing three requirements that would require Responsible Entities to: evaluate their networks within Electronic Security Perimeters and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations; collect, analyze, and respond appropriately to anomalous network communications within applicable networks; and protect the collected internal network security monitoring related network communications data to

[5] *Petition of the N. Am. Elec. Reliability Corp. for Approval of Proposed Reliability Standard CIP-015-1*, Docket No. RM24-7-000 (June 24, 2024) [hereinafter INSM Petition].

prevent unauthorized data manipulation and preserve the data to facilitate additional investigation.[6]

As noted by FERC in the NOPR, proposed Reliability Standard CIP-015-1 provides much needed reliability benefits by enhancing Responsible Entities' ability to detect anomalous or malicious activity and provide information to assist in determining an appropriate response.[7] It would further improve the cyber security posture of industry by providing visibility into east-west communications; thus, improving the probability of detection for anomalous or malicious activity within the Electronic Security Perimeter.[8] Accordingly, proposed Reliability Standard CIP-015-1 should be approved by the Commission without delay so that its reliability benefits may be realized as soon as possible.

B. NERC strongly urges the Commission to provide additional clarity on the scope of the NOPR and what is included within the "CIP-networked environment."

NERC agrees that additional reliability benefits may be realized by extending internal network security monitoring protections to EACMS and PACS outside of the Electronic Security Perimeter; however, NERC requests that the Commission provide additional clarity as to the scope of the NOPR and what is intended to be included as a part of the "CIP-networked environment", as it is not a defined term with a clearly understood meaning within industry.

In the NOPR, the Commission "proposes to direct NERC to develop modifications to proposed Reliability Standard CIP-015-1 that would extend [internal network security monitoring] to include EACMS and PACS outside the electronic security perimeter."[9] FERC explains that "[a]ttacks external to the electronic security perimeter may compromise systems, such as EACMS

6 INSM Petition, Exhibit C Technical Rationale at 2.

7 NOPR at P 13.

8 *See id.*

9 *Id.* at P 21.

or PACS, and then infiltrate the perimeter as a trusted communication . . . ."[10] The Commission further explains that its proposal would "direct NERC to develop modifications to the proposed Reliability Standard to include EACMS and PACS, thereby protecting the reliability and security *of all trust zones of the CIP-networked environment*."[11]

As the Commission considers extending internal network security monitoring to include EACMS and PACS outside the Electronic Security Perimeter in a final rule, NERC strongly urges FERC to provide additional clarity beyond the language of the instant NOPR and Order No. 887[12] on what is intended by the term "CIP-networked environment." The term "CIP-networked environment" is not defined within the instant NOPR, Order No. 887, or the NERC Glossary of Terms.[13] NERC appreciates the Commission providing additional context that the "CIP-networked environment" is intended to include all assets and systems to which the CIP standards apply and may be the targets of attacks;[14] that the inclusion of EACMS and PACS would protect all trust zones of the CIP-networked environment;[15] and that extending internal network security monitoring outside the Electronic Security Perimeter would provide benefits in monitoring, detecting, and collecting malicious code or anomalous activity from attackers moving east-west within the EACMS or PACS network segments of the CIP-networked environment.[16] While the additional context is helpful, more clarity would greatly benefit the expeditious development of a new or revised Reliability Standard.

---

10 *Id.* at P 3.
11 *Id.* at P 14 (emphasis added).
12 *Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys.*, Order No. 887, 182 FERC ¶ 61,021 (2023).
13 INSM Petition, Exhibit C Technical Rationale at 3.
14 NOPR at P 15.
15 *Id.* at P 14.
16 *Id.* at P 20.

During the development of proposed Reliability Standard CIP-015-1, the appropriate scope for the project was the subject of much debate. Early in development, the drafting team considered several alternatives as to what network data flows may be included within internal network security monitoring. For example, in the initial posting, the drafting team proposed a broader scope for the proposed requirements than in the final version. Specifically, the drafting team proposed including routable network communications between EACMS and PACS outside the Electronic Security Perimeter. The drafting team's review of the initial comments, that overwhelmingly argued that the inclusion of EACMS and PACS outside of the Electronic Security Perimeter exceeded the scope of Order No. 887 and what was generally understood to be included with the "CIP-networked environment", demonstrated that the term "CIP-networked environment" is not a well understood term across industry.[17]

To facilitate an expeditious development process, it would be beneficial if the Commission clarifies in a final rule the expected scope of any internal network security monitoring revisions. For example, in extending the CIP-015-1 protections to EACMS and PACS, would the term "CIP-

[17] *See* INSM Petition at pp. 16-17 & notes 58-60; *See, e.g.*, NERC, *Consideration of Comments* – Project 2023-03 Internal Network Security Monitoring, February 2024 (INSM Petition Exhibit F Summary of Development and Complete Record of Development, item 19) comments of Avista Corporation at 121 (stating "[w]e believe the standard is clear for assets within the ESP, however there is room for confusion when assets are located outside the ESP. Specifically, if the PACS is outside the 'CIP-Network Environment' then it should be out of scope as well."); comments of Duke Energy at 61-62 ("[w]e do not support the interpretation that the CIP-networked environment is inclusive of EACMS and PACS-classified cyber assets that do not reside within an ESP."); comment of SMUD at 104 ("[i]ncluding EACMS and PACS, which are not required to be protected by an ESP, Electronic Access Point (EAP), or required to be in a 'trust zone' does not align with intent of the SAR or the FERC Order, which is to perform network monitoring of traffic between devices *within* a trusted zone."); comments of North American Generator Forum (NAGF) at 115-116 (NAGF "would refer the [drafting team] back to Order [No.] 887 in that the network traffic in scope for INSM is communications within an ESP between other Cyber Assets within that "trust zone" also referred to as east west traffic. The inclusion of EACMS and PACS goes beyond the scope of INSM and the current Draft 1 creates confusion as to the intent of the requirements commingling 'Network Security Monitoring' principles which include devices outside of the [Electronic Security Perimeter] or 'trust zones."); comments of Pacific Gas and Electric Company (PG&E) at 99 ("[t]he FERC Order was for 'internal' communications, but the current language does not clearly indicate this and could be interpreted by auditors to include traffic outside of the ESP, such as those to PACS and EACMS outside of the ESP. PG&E recommends to clearly indicate that communications outside of the ESP to devices such as PACS and EACMS are not in scope.").

networked environment" be restricted to east-west communications between EACMS and PACS outside of the ESP? Similarly, would the communications between PACS and controllers and communications to and from EACMS used solely for electronic access monitoring be included?[18]

NERC looks forward to receiving additional guidance in a final rule that will facilitate expeditious development of any future Reliability Standard revisions.

C. NERC requests that the Commission permit at least 12 months for completion of the proposed revisions.

In order to account for the complexity of the directive proposed in the NOPR and the existing high volume of standards projects in development, many of which are on stringent timelines to respond to FERC directives or NERC corporate goals, NERC asks that a minimum of 12 months be allowed for completion of any standards revisions that result from a final rule. NERC standards projects have been increasing in quantity; coinciding with an increasing pace of technology changes in our industry. Many of these projects are identified as high priority with strict timelines as they may be associated with FERC Order directives or NERC corporate goals, which are focused efforts to address known risks to the BPS and are consistent with NERC's long-term strategic areas of focus. NERC and industry have been driving prioritization efforts to assure available resources are focused on the most critical issues. This prioritization effort, within the Standards Development process, identifies those Reliability Standards Projects that must be allocated resources (time, drafting team members) as well how NERC may acceptably lower the resource demands on projects that have not been designated as "high priority."

[18] *See* diagram on page 6 of the draft 1 Technical Rationale; available at https://www.nerc.com/pa/Stand/Project_202303_INSM_DL/2023-03%20Technical%20rationale%20document%20_Dec14_2023.pdf.

As of November 18, 2024,[19] there were 82 outstanding FERC directives being resolved through the Standards Development process.[20] Based on the seven projects in the High Priority queue for 2025, as of November 18, 2024, NERC anticipates that it will take a more than 10,000 total hours for drafting teams to complete these seven projects by end of 2025.[21] In addition, there are 12 additional medium and low priority projects in development as of November 18, 2024 that are anticipated to continue into 2025.[22]

In the NOPR, the Commission proposes to direct NERC to submit the revised Reliability Standard for Commission approval within 12 months of the effective date of a final rule.[23] During Project 2023-03, INSM, the drafting team spent considerable time and effort considering the inclusion of EACMS and PACS outside of the Electronic Security Perimeter. This experience was informative as to the complexity and challenges involved in realizing the directive proposed in the instant NOPR to extend INSM beyond the Electronic Security Perimeter to include EACMS and PACS. Based upon this experience, NERC asks that a minimum of 12 months be allowed to complete the revisions proposed in the NOPR. If additional time in excess of 12 months was allowed for development of revisions to CIP-015, it would facilitate additional development options, including potentially hosting a technical conference near the beginning of the

---

[19] A current list of Standards Development Projects may be found on NERC's webpage at https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx.

[20] Draft 2025-2027 Reliability Standards Development Plan ("RSDP") at p. 2. The 2025-2027 RSDP was endorsed by the NERC Standards Committee at its October 16, 2024 meeting. NERC, Standards Committee Meeting October 16, 2024, agenda Item 10a (Reliability Standards Development Plan 2025-2027) https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Meeting_Agenda_Package-October_16_2024.pdf [hereinafter 2025-2027 RSDP]. The draft RSDP has been updated to reflect completed directives and an additional high priority project that will continue into 2025. The updated draft RSDP, available at https://www.nerc.com/pa/Stand/Standards%20Development%20Plan%20Library/2025-2027%20%20RSDP_Board.pdf, will be considered for approval by NERC Board of Trustees at the December 2024 meeting. Following approval by the NERC Board of Trustees the 2025-2027 RSDP would be filed with FERC.

[21] 2025-2027 RSDP at 6.

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

[23] NOPR at P 21.

development process that would aim to promote efficient development and drafting. It would also afford NERC flexibility to balance limited resources between competing high priority projects.

II. CONCLUSION

NERC appreciates the opportunity to comment on this matter. As discussed above, NERC supports the Commission exploring ways to strengthen cyber security. NERC also requests that the Commission provide additional guidance in the final rule as to the intended scope of its proposal in order to effectuate targeted and expeditious revisions to proposed Reliability Standard CIP-015. Finally, NERC asks that a minimum of 12 months be allowed for completion of any standards revisions that result from a final rule.

Respectfully submitted,

/s/ Sarah P. Crawford

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Counsel
North American Electric Reliability Corporation
1401 H Street NW, Suite 410
Washington, DC 20005
(202) 400-3000
Lauren.perotti@nerc.net
Sarah.crawford@nerc.net
Counsel for the North American Electric Reliability Corporation

Date: November 22, 2024