UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

REQUEST FOR CLARIFICATION OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Pursuant to Rules 212 and 713 of the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Rules of Practice and Procedure, 18 C.F.R. §§ 385.212, 385.713, the North American Electric Reliability Corporation ("NERC") requests clarification of the Commission's June 26, 2025 Order No. 907.[1] In Order No. 907, the Commission approved Reliability Standard CIP-015-1 (Cyber Security-Internal Network Security Monitoring), provided additional clarification of the term "CIP-networked environment,"[2] and directed additional revisions to extend internal network security monitoring to Electronic Access Control or Monitoring Systems ("EACMS")[3] and Physical Access Control Systems ("PACS") outside the Electronic Security Perimeter within 12 months of the effective date of the Final Rule. In this request, NERC seeks clarification of the scope of Order No. 907 with respect to the term CIP-networked environment. NERC seeks this clarification to eliminate ambiguity regarding the intended scope of the Commission's directive and facilitate a timely development process.

---

[1] *Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring*, Order No. 907, 191 FERC ¶ 61,224 (2025).

[2] The term "CIP-networked environment" is not defined in NERC's Glossary of Terms Used in NERC Reliability Standards. It has been used by the Commission in Order No. 907 and in *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems,* Order No. 887, 182 FERC ¶ 61,021 (2023) [hereinafter Order No. 887].

[3] Unless otherwise indicated, terms capitalized in this filing shall have the meaning provided in the *Glossary of Terms used in NERC Reliability Standards*, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

I. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to the following:[4]

Lauren A. Perotti*
Assistant General Counsel
Sarah P. Crawford*
Senior Counsel
North American Electric Reliability Corporation
1401 H Street NW
Suite 410
Washington, D.C. 20005
202-400-3000
Lauren.perotti@nerc.net
Sarah.crawford@nerc.net

Soo Jin Kim*
Vice President, Engineering and Standards
Jamie Calderon*
Director, Standards Development
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560
Soo.jin.kim@nerc.net
Jamie.calderon@nerc.net

II. STATEMENT OF ISSUES FOR CLARIFICATION

Pursuant to 18 C.F.R. § 385.212, NERC seeks clarification on two issues in Order No. 907:

1) NERC requests clarification as to whether the scope of the term CIP-networked environment is intended to include only the communication paths between the CIP devices for monitoring; or does the scope of CIP-networked environment intend to include all communications on the network segment.

2) Order No. 907 states that the term CIP-networked environment is inclusive of communications between PACS and controllers. NERC seeks clarification as to whether this is inclusive of communications between PACS and non-PACS controllers.

III. BACKGROUND

On January 20, 2022, FERC issued a Notice of Proposed Rulemaking ("NOPR")[5] that proposed directing NERC to develop requirements for internal network security monitoring of high and medium impact Bulk Electric System ("BES") Cyber Systems within the Critical

[4] Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of 18 C.F.R. § 385.203(b) to permit the inclusion of more than two people on the service list.

[5] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Notice of Proposed Rulemaking, 178 FERC ¶ 61,038 (2022).

Infrastructure Protection Reliability Standard ("CIP") Reliability Standards. NERC filed comments on the NOPR on March 28, 2022. On January 19, 2023,[6] FERC issued a Final Rule that directed NERC to develop new or modified CIP Reliability Standards that require internal network security monitoring for CIP-networked environments for all high impact BES Cyber Systems with and without external routable connectivity and medium impact BES Cyber Systems with external routable connectivity.[7]

In response to the directives set forth in Order No. 887, NERC established Project 2023-03, Internal Network Security Monitoring (INSM). This project developed a new Reliability Standard, CIP-015-1 (Cyber Security – Internal Network Security Monitoring) that was filed with the Commission on June 24, 2024.[8] During the development of Reliability Standard CIP-015-1, the scope of the proposed internal network security monitoring requirements was the subject of much debate. Early in Project 2023-03, the drafting team considered including network data from EACMS and PACS outside the Electronic Security Perimeter. Drawing on its technical expertise and following consideration of comments, the drafting team determined that the inclusion of network data feeds within the Electronic Security Perimeter complied with the Commission's directives.[9] It further took into account the language in Order No. 887 that internal network security monitoring should be applied within a trust zone, "such as the electronic security

6 Order No. 887, 182 FERC ¶ 61,021.

7 Order No. 887 at PP 1, 49.

8 *See Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-015-1*, Docket No. RM24-7-000 (June 24, 2024) [hereinafter INSM Petition].

9 INSM Petition at p. 16.

perimeter",[10] and that for the purpose of Order No. 887, "the trust zone applicable to [internal network security monitoring] is the CIP-networked environment."[11]

On September 19, 2024 FERC issued a NOPR that proposed to approve Reliability Standard CIP-015-1 noting that the Reliability Standard will augment responsible entities' ability to detect anomalous or malicious activity and provide information to assist in determining an appropriate response.[12] In the September 2024 NOPR, the Commission sought comments on its proposal to direct NERC "to develop modifications to proposed Reliability Standard CIP-015-1 that would extend INSM to include EACMS and PACS outside the electronic security perimeter."[13]

On November 22, 2024 NERC submitted comments in response to the September 2024 NOPR that: (1) supported FERC's proposal to approve proposed Reliability Standard CIP-015-1; (2) urged the Commission to provide additional clarity on the scope of the term "CIP-networked environment"; and (3) asked that the Commission permit at least 12 months for completion of any proposed revisions.[14]

On June 26, 2025, FERC issued a Final Rule approving Reliability Standard CIP-015-1, Cyber Security – Internal Network Security Monitoring, providing additional clarity of the term CIP-networked environment, and directing NERC to develop modifications to Reliability Standard

---

[10] INSM Petition at p. 16 (citing Order No. 887 at P 2 & n.7 ("An electronic security perimeter is 'the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol'." NERC Glossary)).

[11] INSM Petition at p. 16 (citing Order No. 887 at P 2).

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

[13] *Id.* at P 21.

[14] *See Comments of the N. Am. Elec. Reliability Corp. in Response to Notice of Proposed Rulemaking*, Docket No. RM24-7-000 (Nov. 22, 2024).

CIP-015-1 to extend internal network security monitoring to include EACMS and PACS outside the Electronic Security Perimeter within 12 months of the effective date of the Final Rule.[15]

IV. CLARIFICATION OF "CIP-NETWORKED ENVIRONMENT" PROVIDED IN ORDER NO. 907

In Order No. 907, the Commission clarified that the term CIP-networked environment does not cover all of a responsible entity's network.[16] Specifically, the Commission stated that:

> [T]he scope of 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.[17]

The Commission found that the described 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[18] to undertake any number of malicious acts as described in Order No. 887."[19] The Commission further explained that implementation of internal network security monitoring "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."[20] Order No. 907 included the below

---

15 *See* Order No. 907.

16 *Id.* Order at P 43.

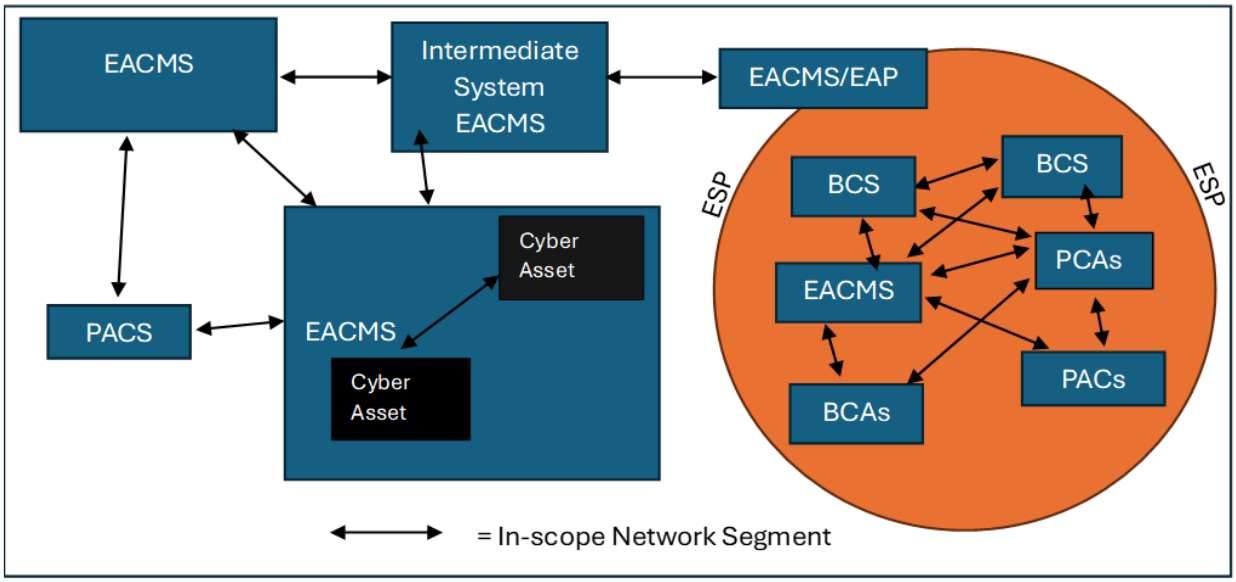
17 *Id.*

18 *Id.* at P 43 n. 83 (citing 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).

19 *Id.* at P 43 n. 84 (citing 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).")).

20 *Id.* at P 43.

graphic depicting 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 requirements of this final rule.[21]



Order No. 907 additionally provided that the term CIP-networked environment is "inclusive of EACMS and PACS necessary to protect all trust zones of the term[22] and extends beyond the electronic security perimeter to guard against attackers moving east-west within the EACMS or PACS network segments of the term."[23] The Commission stated that "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."[24] The Commission further stated that "communication between PACS and controllers and communications to and from EACMS used solely for electronic access monitoring are

21 *Id.*

22 *Id.* at P 44 n. 85 (citing Order No. 887, 182 FERC ¶ 61,021 at P 14).

23 *Id.* at P 44 n. 86 (citing NIST SP 800-215 at 5; NSA Network Security Guide at 3).

24 *Id.* at P 45.

included in the term CIP-networked environment."[25]

V. REQUEST FOR CLARIFICATION

NERC appreciates the clarification of the term CIP-networked environment that is provided by the Commission in Order No. 907. NERC, however, believes that additional clarity with respect to the scope of the term CIP-networked environment is needed to facilitate an efficient standards development process. First, NERC seeks additional clarity as to whether the scope of the term CIP-networked environment is intended to include only the communication paths between the CIP devices for monitoring; or whether it is intended to include all communications on the network segment for monitoring. Second, Order No. 907 states that the term CIP-network environment is inclusive of communications between PACS and controllers; NERC seeks clarification as to whether this is inclusive of communications between PACS and non-PACS controllers.[26] Addressing these questions about the intended scope of Order No. 907 will provide the drafting team a clear direction, thus promoting a timely development process that develops revisions that are responsive to the Commission's intent.

In the Final Rule, the Commission clarifies that the CIP-networked environment includes the systems within the Electronic Security Perimeter and at least one of the following: (1) network segments 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.[27] The Commission also includes a graphic in its discussion to demonstrate the scope of

---

25 *Id.*

26 *Id.*

27 *Id.* at P 43.

the CIP-networked environment.[28] The graphic does not show non-CIP cyber assets outside of the Electronic Security Perimeter as within scope; however, in the text above the graphic, Order No. 907 expressly includes "network segments that are connected to EACMS and PACS outside of the electronic security perimeter".[29] NERC thus seeks clarification as to whether the scope of the term CIP-networked environment is intended to include only the communication paths between the CIP devices for monitoring; or is it intended to include all communications on the network segment.

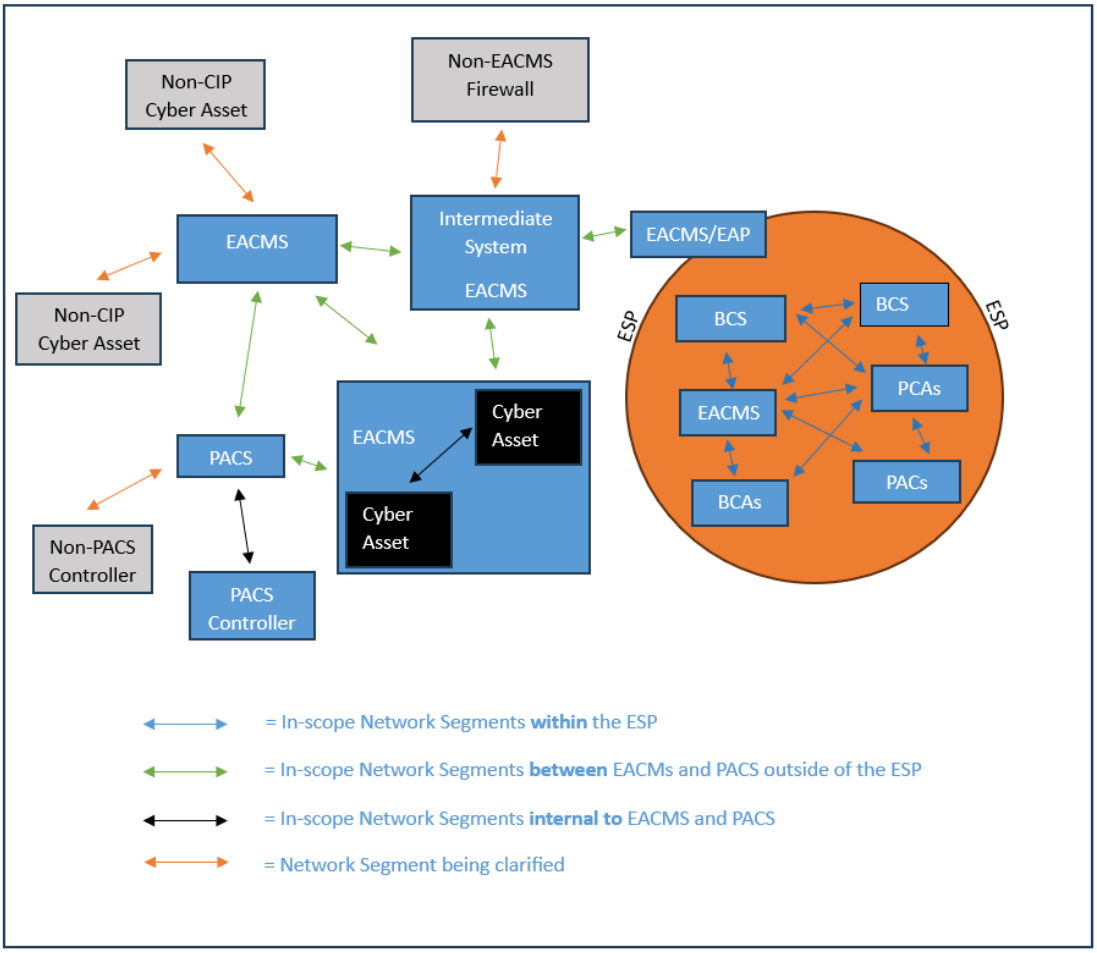
As shown in the graphic below, NERC understands the scope of the term CIP-networked environment to include the following: (1) the systems within the Electronic Security Perimeter (represented with blue arrows in the graphic); (2) network segments between EACMs and PACS outside of the Electronic Security Perimeter (represented with green arrows in the graphic); and (3) network segments internal to EACMs and PACS outside of the Electronic Security Perimeter (represented with black arrows in the graphic). The graphic that is included within the Commission's clarification of the term CIP-networked environment, however, appears to include communication paths, not necessarily network segments. Thus, NERC seeks to clarify whether the scope of the term CIP-networked environment is intended to include the communication paths between the CIP devices, indicated by the blue, black and green arrows in the graphic below; or is it intended to include all communications on the network segments indicated by all arrows in the graphic below, including orange arrows.

To further illustrate the requested clarification, NERC provides the following graphic:

---

28 *Id.*

29 *Id.*



NERC seeks clarification with respect to whether the orange arrows between the blue and gray boxes represented in the graphic above are intended to be included within the scope of CIP-networked environment and thus monitored.

In addition, Order No. 907 states that "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".[30] NERC seeks clarification as to whether this is inclusive of communications between PACS and non-PACS controllers.

VI. CONCLUSION

For the reasons set forth in this filing, NERC requests that FERC issue

[30] Order No. 907 at P 45.

an Order granting the Request for Clarification as set forth above.

Respectfully submitted,

/s/ Sarah P. Crawford

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Senior Counsel
North American Electric Reliability Corporation
1404 H Street, N.W., 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: July 25, 2025

CERTIFICATE OF SERVICE

I hereby certify that on this 25th day of July, 2025, I have served a copy of the foregoing document on the official service list compiled by the Office of the Secretary for the above referenced proceeding.

/s/ Sarah P. Crawford

Lauren Perotti
Assistant General Counsel
Sarah P. Crawford
Senior Counsel
North American Electric Reliability Corporation
1404 H Street, N.W., Suite 410
Washington, DC 20005
(202) 400-3000
lauren.perotti@nerc.net
sarah.crawford@nerc.net
Counsel for the North American Electric Reliability Corporation