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

REQUEST FOR CLARIFICAITON OF THE EDISON ELECTRIC INSTITUTE AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

Pursuant to section 313 of the Federal Power Act ("FPA")[1] and Rules 212 and 713 of the Rules of Practice and Procedure of the Federal Energy Regulatory Commission ("Commission" or "FERC"),[2] the American Public Power Association ("APPA"), Edison Electric Institute ("EEI") and the National Rural Electric Cooperative Association ("NRECA") (together, the "Trade Associations") hereby request clarification of Order No. 907, issued in the above-captioned proceeding on June 26, 2025.[3] The Trade Associations filed timely comments in this proceeding on November 26, 2024, in response to the Commission's September 19, 2024, Notice of Proposed Rulemaking ("NOPR").[4] In their comments on the NOPR, the Trade Associations sought additional clarity regarding the term "CIP-networked environment," noting the diversity of implemented network architectures.[5] As further discussed herein, the Trade Associations seek clarification that Order No. 907 is not intended to be interpreted to extend the scope of CIP-015-1 to require monitoring of network traffic between certain assets outside of the Electronic Security Perimeter ("ESP"), specifically network traffic between corporate assets not subject to the NERC CIP Standards and certain Electronic Access Control or Monitoring Systems

[1] 16 U.S.C. § 825l.
[2] 18 C.F.R. §§ 385.212, 385.713.
[3] Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring, 191 FERC ¶ 61,224 (2025) ("Order No. 907").
[4] Comments of American Public Power Association, et al. in response to Notice of Proposed Rulemaking under FERC Docket No. RM24-7-000, Accession No. 20241126-5299 (filed Nov. 26, 2024).
[5] *Id.* at p. 8.

("EACMS") identified as Intermediate Systems. Further, the Trade Associations seek clarification that Order No. 907 is intended to be interpreted to extend the scope of CIP-015-1 to require monitoring of network traffic between PACS including PACS controllers, and not a broader definition of the term "controller."

I. BACKGROUND

In Order No. 887, the Commission directed NERC to develop "new or modified CIP Reliability Standards requiring INSM for the CIP-networked environment for all high impact [Bulk Electric System ("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."[6] The Commission observed that internal network security monitoring ("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."[7]

The Commission found that the Reliability Standard developed in response to Order No. 887 did not fully implement the scope of protection the Commission contemplated.[8] As a result and to address the gap, the Commission issued the NOPR and proposed to "direct NERC to develop modifications to the proposed Reliability Standard to include EACMS and PACS, thereby protecting the reliability and security of all trust zones of the CIP-networked environment."[9]

---

[6] Internal Network Sec. Monitoring for High & Medium Impact Bulk Elec. Sys. Cyber Sys., 182 FERC ¶ 61,021 at P 3 (2023) ("Order No. 887").
[7] *Id.* at P 2.
[8] Critical Infrastructure Protection Reliability Standard CIP-015-1 – Cyber Security – Internal Network Security Monitoring, Notice of Proposed Rulemaking, 188 FERC ¶ 61,175 at P 14 (Sept. 19, 2024).
[9] *Id.*

In Order No. 907, FERC noted that "the 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."[10] It also included a graphic depicting the CIP-networked environment.[11] Further, in response to NERC's questions, FERC states that "communication between PACS and controllers … are included in the term CIP-networked environment."[12]

The Trade Associations seek clarification with respect to language in Order No. 907 regarding the scope of CIP-015-1, as further described below.

II. REQUEST FOR CLARIFICATION

As noted, the Commission directed NERC to revise the scope of CIP-015-1 to include, among other things, network segments that are connected to EACMS and PACS outside of the electronic security perimeter.[13] The Trade Associations seek clarification that Order No. 907 is not intended to be interpreted to extend the scope of CIP-015-1 to require monitoring of network traffic between non-CIP assets and EACMS and PACS outside of the ESP. Specifically, the Trade Associations request clarification that CIP-015-1 does not require monitoring of network traffic between non-CIP assets and Intermediate Systems that are classified as EACMS.

The language in Paragraph 43 of Order No. 907 references "network segments that are connected to EACMS and PACS outside of the electronic security perimeter," which could be

[10] Order No. 907 at P 43.
[11] *Id.* at p. 26.
[12] *Id.* at P 45.
[13] *Id.* at P 43.

interpreted as a requirement to monitor network segments between non-CIP assets and Intermediate Systems. Intermediate Systems are a type of EACMS located outside of the ESP that perform access control to restrict Interactive Remote Access to only authorized users.[14] The Commission's graphic included in Order No. 907 suggests that FERC's intended scope would only require monitoring of network segments between EACMS and PACS outside of the ESP, and would not include monitoring of network segments between non-CIP assets and Intermediate Systems. While the graphic is consistent with the Trade Associations' understanding, we seek clarification to confirm this interpretation.

Additionally, the Commission responded directly to questions posed by NERC[15] regarding scoping and stated that "communications between PACS and controllers… are included in the CIP-networked environment."[16] The Commission's graphic included in Order No. 907 suggests that use of the term "controllers" was intended to include controllers classified as PACS and EACMS, and not a broader, more generic definition of controller that would expand scope to non-CIP assets. This is consistent with the Trade Associations' understanding, and we seek clarification to confirm this interpretation.

In furtherance of this request for clarification, the Trade Associations respectfully ask that the Commission establish a joint FERC and NERC technical conference or workshop on the implementation of Order No. 907. A technical conference or workshop would support the industry in achieving the intended security outcomes of Order No. 907 in an efficient manner.

[14] North American Electric Reliability Corporation, *Glossary of Terms Used in Reliability Standards*, latest revision dated January 7, 2025.
[15] Comments of the North American Electric Reliability Corporation in response to Notice of Proposed Rulemaking under FERC Docket No. RM24-7-000, Accession No. 20241122-5055 (filed Nov. 22, 2024).
[16] Order No. 907 at P 45.

III. CONCLUSION

The Trade Associations respectfully request that the Commission grant this request for clarification consistent with the views expressed above.

Respectfully submitted,

_____
Andrea Koch
Senior Director, Reliability Policy
202.508.5484
akoch@eei.org

Kristine Martz
Director, Reliability Policy
202.508.5730
kmartz@eei.org

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

_____
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

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

John Ransom
Director of Regulatory Affairs, Grid Security

John.Ransom@nreca.coop

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

July 25, 2025

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 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.

Dated this 25th day of July 2025.

/s/ Sandra S. Osborn
Sandra S. Osborn
Deputy General Counsel
ssafro@eei.org
(202) 508-5129

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