UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

| | |
|---|---|
| Critical Infrastructure Protection Reliability Standard CIP-003-11 – Cyber Security – Security Management Controls | Docket No. RM25-8-000 |

**COMMENTS OF THE TRADE ASSOCIATIONS**

The American Public Power Association (APPA), Edison Electric Institute (EEI), Electric Power Supply Association (EPSA), Large Public Power Council (LPPC), National Rural Electric Cooperative Association (NRECA), and Transmission Access Policy Study Group (TAPS) (together, the Trade Associations) respectfully submit these comments in response to the Federal Energy Regulatory Commission's (Commission) September 18, 2025, Notice of Proposed Rulemaking (NOPR)[1] proposing to approve Critical Infrastructure Protection (CIP) Reliability Standard CIP-003-11 (Cyber Security – Security Management Controls) submitted by the North American Electric Reliability Corporation (NERC).

The Trade Associations support the NOPR's proposal to approve CIP-003-11 without any further directives. We also comment on the Commission's request for additional information on the continuing evolution of threats of compromise to low impact Bulk Electric System (BES) Cyber Systems. Finally, we urge the Commission not

[1] Critical Infrastructure Protection Reliability Standard CIP-003-11 – Cyber Security – Security Management Controls, 192 FERC ¶ 61,227 (2025).

to direct NERC to conduct an additional study given significant efforts underway at NERC to evaluate those risks.[2]

## IDENTIFICATION OF FILING PARTIES

**APPA** is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. Public power utilities are in every state except Hawaii. They collectively serve over 55 million people in 49 states and five U.S. territories, and account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers. Public power utilities are load-serving entities, with the primary goal of providing the communities they serve with safe, reliable electric service at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities.

**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 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

---

[2] In these comments, undefined capitalized terms—such as Cyber Systems or Cyber Assets—are used as defined in the NERC Glossary of Terms. *See* NERC, Glossary of Terms Used in NERC Reliability Standards (Nov. 5, 2025), https://www.nerc.com/globalassets/standards/reliability-standards/glossary_of_terms_111225.pdf.

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 ISOs/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 serve 42 million people (one of every eight electric consumers), powering 22 million businesses, homes, schools and farms in 48 states and across 56 percent of the nation's landmass.[3]

---

[3] The facts and figures in this description of NRECA member cooperatives, and their sources, are posted on the NRECA public website. See https://www.electric.coop/electric-cooperative-fact-sheet (visited

**TAPS** is an association of transmission-dependent utilities (TDUs) in thirty-five states promoting open and non-discriminatory transmission access. TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the Bulk Power System and are highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards.

## COMMUNICATION

All correspondence, communications, pleadings, and other documents related to this proceeding should be addressed to the undersigned individuals. The Trade Associations request that the Commission waive Rule 203(b)(3), 18 C.F.R. § 385.203(b)(3), to allow each of the individuals listed below to be placed on the official service list in this proceeding to avoid delays in receipt of notices and responses to pleadings.

## COMMENTS

### A. CIP-003-11 REDUCES THE RISK ASSOCIATED WITH COORDINATED ATTACKS ON LOW IMPACT BES CYBER SYSTEMS.

In October 2022, NERC staff and industry subject-matter experts—including several members of the Trade Associations—issued a comprehensive review and analysis of risks presented by various facilities that meet the criteria for low impact BES Cyber Systems.[4] The report reaffirmed that most individual BES Cyber Systems should be

---

September 5, 2025).

[4] NERC, Low Impact Criteria Review Report (Oct. 2022), https://prod.nerc.com/globalassets/our-

treated as low impact, given that the assets they support are also of low impact individually.[5] The primary risk presented by low impact BES Cyber Systems, the report concluded, is not from attacks on individual systems but rather from a coordinated attack across many individual low impact BES Cyber Systems affecting multiple BES assets.[6]

The overall risk associated with low impact BES Cyber Systems—individually and collectively—must be assessed by considering both the likelihood of a successful attack and the expected impact of a successful attack. While the expected aggregate impact of a coordinated attack on multiple low impact BES Cyber Systems could, indeed, be equivalent to the expected impact of an attack on a single medium impact BES Cyber System, the likelihood of successfully compromising multiple low impact BES Cyber Systems is lower. The vast variety of asset types, system configurations, and operating environments that comprise low impact BES Cyber Systems adds to the complexity—and hence lowers the likelihood—of a successful coordinated attack.

NERC's October 2022 report evaluated a variety of coordinated attack methods using an impact-likelihood framework and concluded that the highest risk to the BES is from unauthorized remote access to low impact BES Cyber Systems.[7] To mitigate that risk, the report recommended revising the CIP standards for low impact BES Cyber

---

work/reports/white-papers/nerc_licrt_white_paper_clean.pdf.

[5] *Id.* at 5. This is consistent with the longstanding design of the BES to withstand the loss of any individual asset. *Id.* at 15.

[6] The report defined a "coordinated attack" as "an orchestrated attack against multiple low impact BES Cyber Systems, independent of Responsible Entity ownership, which has the goal of causing an Adverse Reliability Impact to the BES." *Id.* at 5.

[7] *Id.* at 6.

Systems to require remote user authentication, protection of user authentication information, and detection of malicious communications.[8]

NERC's proposed CIP-003-11 standard appropriately implements those recommendations by requiring entities responsible for a low impact BES Cyber System to (1) permit only necessary electronic access, (2) detect malicious communication, (3) authenticate users, (4) protect user authentication information, and (5) control vendor electronic access. Collectively, these new requirements for low impact BES Cyber Systems will reduce the likelihood of a successful coordinated attack.

Trade Associations therefore support the NOPR's proposal to approve CIP-003-11.

## B. THE EXISTING CIP STANDARDS EFFECTIVELY MITIGATE RISK ASSOCIATED WITH LATERAL MOVEMENT FROM LOW IMPACT BES CYBER SYSTEMS TO MEDIUM AND HIGH IMPACT BES CYBER SYSTEMS.

The NOPR identifies a separate category of risk associated with low impact BES Cyber Systems: lateral movement.[9] Analytically, the threat of lateral movement should be evaluated separately for (a) movement from a compromised low impact BES Cyber System to a medium or high impact BES Cyber System, and (b) movement from a compromised non-BES Cyber Asset to low impact BES Cyber System.

The existing suite of CIP standards has long been designed to address the first category of lateral movement threats. Medium and high impact BES Cyber Systems have

---

[8] *Id.* at 15.

[9] NOPR at P 15.

a robust suite of requirements that ensure, as a baseline, lateral movement threats are mitigated.

Consider, as a starting point, the requirements in CIP-005 to establish an Electronic Security Perimeter around the entire network to which a medium or high impact BES Cyber System is connected. All connectivity to such a network must be through an identified Electronic Access Point which must by default deny access to the network unless permission is explicitly granted, including a reason for granting access.[10] Furthermore, CIP-005 requires any Interactive Remote Access sessions to utilize Intermediate Systems, use encryption, and require multi-factor authentication.[11]

If a low impact BES Cyber System (or a non-BES Cyber Asset) resides on the same network as a medium or high impact BES Cyber System, those electronic access requirements apply to all assets on the network, mitigating lateral movement threats. And, where a utility has implemented network segmentation, a medium or high impact BES Cyber System is protected against lateral movement threats from any low impact BES Cyber System outside the Electronic Security Perimeter.

In addition to the requirements of CIP-005, the full suite of CIP standards provides defense-in-depth against the kind of lateral movement threats identified by the NOPR. Requirements for system security management, configuration change management, information protection, and—most recently—internal network security monitoring collectively ensure that medium and high impact BES Cyber Systems have

---

[10] *See* CIP-005-7 (Cyber Security – Electronic Security Perimeters), Requirement R1.

[11] *See* CIP-005-7 (Cyber Security – Electronic Security Perimeters), Requirement R1.

baseline protection against threats emanating from a compromised low impact BES Cyber System.

Furthermore, Trade Associations' members actively engage in cyber security protections above and beyond what is required by the CIP standards. These protective measures include strategic partnerships and information sharing, robust architecture, aggressive active threat hunting, drills and exercises and continuous penetration testing, and resiliency measures.

### C. CIP-003-11 PROVIDES ADEQUATE MITIGATION TO PREVENT LATERAL MOVEMENT FROM NON-BES CYBER ASSETS TO LOW IMPACT BES CYBER SYSTEMS.

The NOPR gives examples of threat actors that "leveraged the trust of less protected systems to move laterally and pivot, compromising externally connected, higher criticality targets."[12] As noted above, the risk of this type of tactic applied against medium and high impact BES Cyber Systems has long been mitigated by the existing CIP standards. So, it is unsurprising that the NOPR's examples do not involve medium or high impact BES Cyber Systems.

With respect to low impact BES Cyber Systems, the existing CIP standards require basic protections that reduce the risk of lateral movement from non-BES Cyber Assets. For example, the currently enforceable CIP-003-8 standard requires responsible entities implement electronic access controls that permit only necessary communication between a low impact BES Cyber System and a Cyber Asset outside the asset containing

---

[12] NOPR at P 15.

the low impact BES Cyber System.[13] And Trade Association members often implement protections for their low impact BES Cyber Systems that go beyond that baseline requirement.

NERC's proposed CIP-003-11 will require responsible entities to implement more robust electronic access protections for low impact BES Cyber Systems. These new requirements that address the threat of coordinated attacks on multiple low impact BES Cyber Systems also have the effect of mitigating against lateral movement threats.

The NOPR seems to suggest that the new CIP-003-11 requirements do not require a responsible entity to restrict access to Cyber Assets that are on the same network as a low impact BES Cyber System.[14] In fact, CIP-003-11 does require a responsible entity to implement electronic access controls to the entire network that contains a low impact BES Cyber System, including any non-BES Cyber Assets that reside on that network. The requirements of Section 3.1 of the standard apply to the entire "asset containing the low impact [BES Cyber System]" and Sections 3.1.3 and 3.1.4 specifically require authentication of every user with access to the "network(s) containing low impact [BES Cyber Systems]."[15] In the unusual situation where a network containing a low impact BES Cyber System expanded beyond the boundary of a particular asset, a responsible entity could attempt to argue that it is not strictly required to control access to network assets outside the asset. However, the diagrams accompanying the text illustrate the

---

[13] CIP-003-8 (Cyber Security – Security Management Controls), Attachment 1, Section 3.1.

[14] NOPR at P 15 ("an entity is not required to authorize and restrict electronic access to any other Cyber Asset that is on the same network as the low impact BES Cyber System, thereby putting the low impact BES Cyber System at a greater risk of compromise.").

[15] CIP-003-11, Attachment 1, Section 3.1.

drafting team's intent to protect all Cyber Assets on a network that contains a low impact BES Cyber System, so such an interpretation should not be viewed as valid.[16]

The NOPR also states that CIP-003-11 does not require an entity to "respond to or mitigate the risk of compromise to its low impact BES Cyber Systems."[17] In fact, CIP-003-11 requires a complementary set of security controls to protect, detect, and respond to threats to low impact BES Cyber Systems.[18] For example, Section 3.1.1 requires a responsible entity to protect assets by preventing unnecessary unauthorized access. Section 3.1.2 requires detection of unauthorized electronic access. And Section 4 requires responsible entities to implement an incident response plan that includes responding to and reporting on Cyber Security Incidents. In short, CIP-003-11 *does* require each responsible entity to "respond to [*and*] mitigate the risk of compromise to its low impact BES Cyber Systems."

### D. A FERC DIRECTIVE TO CONDUCT A FURTHER STUDY IS UNWARRANTED BECAUSE NERC AND INDUSTRY ARE CURRENTLY ENGAGED IN SEVERAL EFFORTS TO FURTHER IMPROVE CYBERSECURITY OF LOW IMPACT SYSTEMS TO ADDRESS EVOLVING THREATS.

The NOPR asks whether it is worthwhile to direct NERC to perform a study on evolving threats to low impact BES Cyber Systems.[19] The Trade Associations and their members have actively collaborated—and will continue to collaborate—with NERC and

---

[16] See NERC Petition, Exhibit 6 (Technical Rationale) at 4-11, Figures 1-5 and accompanying text (illustrating how the drafting team interpreted the requirements of Section 3.1).

[17] NOPR at P 15.

[18] *See* National Institute of Standards and Technology, NIST Cybersecurity Framework (CSF) 2.0 at 3-4 (2004), https://doi.org/10.6028/NIST.CSWP.29 (describing the core functions as govern, identify, protect, detect, respond, and recover).

[19] NOPR at P 16.

all other stakeholders to continue assessing cybersecurity risks to the BES and continuously improve best security practices to protect the grid against evolving threats. To avoid duplicating the multiple ongoing efforts by NERC and industry to evaluate the issues identified in the NOPR, the Trade Associations urge the Commission to refrain from directing NERC to conduct an additional study at this time.

Several such actions are already underway. Notably, in December 2024, the NERC Board of Trustees approved a priority work plan item for NERC staff to develop a CIP roadmap for ensuring CIP standards provide a baseline protection for an evolving risk environment.[20] This roadmap effort, which Trade Association members have been actively supporting, includes an evaluation of emerging risks, including network intrusion, new registrants, emerging threats, cloud usage, and artificial intelligence.[21]

Additionally, Trade Association members are leading several efforts through NERC's Reliability and Security Technical Committee to better understand emerging risks and develop best practices for mitigating them. Those efforts include:[22]

- Developing a report titled "AI Benefit and Risk Assessment for the BPS."
- Developing a whitepaper or security guideline for synchrophasors.
- Developing a new security guideline on vendor incident response.
- Revising the existing security guidance document on procurement language.

---

[20] NERC, Board of Trustees Meeting Minutes for December 2024, at Agenda Item 6 - 2025 Work Plan Priorities (Dec. 10, 2024) (describing Workplan Priority #3 as "Create a roadmap for ensuring CIP standards provide baseline protection for an evolving risk environment.").

[21] *Id.*

[22] NERC, Reliability and Security Technical Committee Work Plan at lines 69, 71, 74, 77, 78 (Oct. 28, 2025), https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/rstc-work-plan.xlsx.

- Revising the existing security guidance document on cloud solutions and encryption of BES Cyber System Information.

Moreover, Trade Association members are working closely with NERC on five new standards development projects that will enhance the overall security of the BES:

- 2023-09 Risk Management for Third-party Cloud Services
- 2022-05 Modifications to CIP-008 Reporting Threshold
- 2025-02 Internal Network Security Monitoring Standard Revision
- 2025-06 Supply Chain Risk Management
- 2021-03 CIP-002

In short, NERC and the industry are working tirelessly by improving mandatory reliability standards, developing best practices, and investing in best-in-class cybersecurity protections. Given the extensive efforts already underway, Trade Associations agree with comments filed by NERC urging the Commission not to direct such an additional study at this time.

## CONCLUSION

Maintaining the security of the grid in the face of evolving cyber threats remains a top priority for the Trade Associations and their members. NERC's proposed CIP-003-11 reliability standard will improve the baseline cybersecurity requirements to mitigate against threats of a coordinated attack on multiple low impact BES Cyber Systems. The proposed reliability standard, in conjunction with the full suite of CIP standards, also provides effective mitigation against threats of lateral movement between BES Cyber Systems. The Commission should therefore (1) approve CIP-003-11, and (2) refrain from directing NERC to conduct any additional studies at this time.

Respectfully submitted,

**American Public Power Association**

*/s/ Latif M. Nurani*
Desmarie Waterhouse
Latif M. Nurani
AMERICAN PUBLIC POWER ASSOCIATION
2541 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
dwaterhouse@publicpower.org
lnurani@publicpower.org

**Edison Electric Institute**

*/s/ Andrea Koch*
Andrea Koch
Senior Director, Reliability Policy
EDISON ELECTRIC INSTITUTE
701 Pennsylvania Avenue NW
Washington, DC 20004
(202) 508-5000
akoch@eei.org

**Electric Power Supply Association**

*/s/ Nancy Bagot*
Nancy Bagot
Senior Vice President
Bill Zuretti,
Director, Regulatory Affairs & Counsel
ELECTRIC POWER SUPPLY ASSOCIATION
1401 New York Avenue NW
Suite 950
Washington, DC 20005
(202) 628-8200
nancyb@epsa.org
bzuretti@epsa.org

**Large Public Power Council**

*/s/ Jonathan D. Schneider*
Jonathan D. Schneider
John E. McCaffrey
STINSON LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 785-9100
jonathan.schneider@stinson.com
john.mccaffrey@stinson.com

*Attorneys for LPPC*

**National Rural Electric Cooperative Association**

*/s/ Mary Ann Ralls*
Mary Ann Ralls
Senior Director, Regulatory Affairs
Patti Metro
Senior Director, Grid Operations & Reliability
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
4301 Wilson Boulevard
Arlington, VA 22203
maryann.ralls@nreca.coop
patti.metro@nreca.coop

**Transmission Access Policy Study Group**

*/s/ Cynthia S. Bogorad*
Cynthia S. Bogorad
Lauren L. Springett
Samuel B. Whillans
SPIEGEL & MCDIARMID LLP
1818 N Street NW, 8th Floor
Washington, DC 20036
(202) 879-4000
cynthia.bogorad@spiegelmcd.com
lauren.springett@spiegelmcd.com
samuel.whillans@spiegelmcd.com

*Attorneys for TAPS*

November 24, 2025