UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls	)	**Docket No. RM17-11-000**

COMMENTS OF
THE AMERICAN PUBLIC POWER ASSOCIATION, EDISON ELECRIC INSTITUTE AND NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

I. INTRODUCTION

The American Public Power Association ("APPA"), Edison Electric Institute ("EEI") and National Rural Electric Cooperative Association ("NRECA") (together, the "Trade Associations") on behalf of our member companies, hereby respectfully submit comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") on October 19, 2017, in the above-referenced docket.[1]

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities are located in every state except Hawaii. They collectively serve over 49 million people and account for 15 percent of all sales of electric energy (kilowatt-hours) to ultimate customers. 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

[1] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 161 FERC ¶ 61,047 (2017) ("NOPR").

stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities. Approximately 264 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 60 international electric companies, with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums. EEI's U.S. members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to the mandatory Reliability Standards developed by the North American Electric Reliability Corporation ("NERC") and enforced by NERC and the Commission.

NRECA represents the interests of the nation's more than 900 rural electric utilities responsible for keeping the lights on for more than 42 million people across 47 states. Electric cooperatives are driven by their purpose to power communities and empower their members to improve their quality of life. Affordable electricity is the lifeblood of the American economy, and for 75 years electric co-ops have been proud to keep the lights on. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve. Additionally, NRECA's members participate in all of the organized wholesale electricity markets throughout the country. And for this reason, NRECA participates in a variety of Commission proceedings,

rulemakings and notices of inquiries on behalf of its members affecting the reliability of the BES.

Accordingly, the members of the Trade Associations are directly affected by the NOPR. As discussed herein, the Trade Associations support the Commission's proposal in its NOPR to approve Reliability Standard CIP-003-7 ("Proposed Standard" or "CIP-003-7"). The Trade Associations agree with the Commission that the Proposed Standard will improve the baseline cybersecurity posture of responsible entities compared to CIP-003-6. However, the Trade Associations do not support the additional modifications proposed by the Commission in the NOPR and encourage prompt action by the Commission to approve the Proposed Standard without modification.

II. COMMENTS

Four years ago, in Order No. 791, the Commission directed NERC to modify the CIP Standards to "address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity's protections for low impact assets."[2] The order did not require NERC to develop specific controls for low impact facilities,[3] but required that the criteria "should be clear, objective, commensurate with their impact on the system, and technically justified."[4] NERC responded with version 6 of CIP-003, which requires responsible entities[5] to implement cybersecurity plans for assets with low impact systems to meet specific security

[2] Order No. 791 at P 106.

[3] *Id*.

[4] *Id*. at P 110.

[5] This includes responsible entities that own multiple levels of impact systems and those that own only low impact systems.

objectives related to awareness, physical security, electronic access, and incident response.[6] Two years later, in Order No. 822, the Commission acknowledged that version 6 would improve the baseline security posture of applicable entities,[7] but directed NERC to further modify this standard to clarify the electronic access control obligations and to address the risks posed by transient electronic devices to low impact BES Cyber Systems. NERC responded with CIP-003-7, which is the seventh version of CIP-003 and the subject of this NOPR.

In the NOPR, the Commission, consistent with Order Nos. 791 and 822, proposes to approve the Proposed Standard and direct NERC to further modify it. Specifically, the Commission proposes to direct NERC to modify the electronic access control requirements in Section 3 of CIP-003-7 and the third-party managed transient cyber asset requirements in Section 5.2 of CIP-003-7.

The Trade Associations do not support the proposed modifications for the reasons discussed in greater detail below and encourage the Commission to approve the Proposed Standard without modification. Importantly, the Proposed Standard addresses the ambiguity identified by the Commission in Order No. 822 by retaining the security objective from CIP-003-6, while giving responsible entities additional tools to achieve that objective. Despite meeting those objectives, the proposed modifications, if ordered, would result in the drafting, approval and implementation of version 8 of CIP-003 shortly after implementation of version 7.

Section 3 of Attachment 1 of the Proposed Standard should not be modified because it gives responsible entities needed flexibility to develop and implement effective electronic access

[6] Order No. 822 at P 10.

[7] *Id*. at P 2.

controls for low impact BES Cyber Systems. Section 5.2 of Attachment 1 of the Proposed Standard should not be modified to explicitly require risk mitigation of third-party transient cyber asset risk because responsible entities are already obligated to achieve the objective of "mitigating risk" as part of the over-arching obligations set forth in Section 5.

Also, approving the Proposed Standard for implementation at the same time as directing further modifications will create inefficient and unnecessary burdens on responsible entities as these entities will have to undertake efforts to achieve compliance with the approved Sections 3 and 5.2 as soon as the Commission issues a Final Rule and, when that implementation effort is complete, be faced with an immediately subsequent implementation effort for the directed modifications.

A. The Commission should not direct modifications to the Section 3 electronic access control requirements because the Proposed Standard provides responsible entities the flexibility needed to develop and implement effective controls to restrict electronic access to low impact BES Cyber Systems.

The Commission proposes to direct NERC to modify the electronic access control requirements in CIP-003-7[8] to provide clear, objective criteria to reduce the deference afforded responsible entities in developing their electronic access controls for their low impact facilities[9] and to provide auditors adequate information to assess the reasonableness of the responsible entities identification of which communications are necessary and how electronic access was restricted.[10] The Commission references the high and medium impact system electronic access controls in CIP-005 and CIP-007 as a possible model[11] and is concerned that the CIP-003

[8] Section 3.1 of Attachment 1 of the proposed Reliability Standard CIP-003-7.

[9] NOPR at P 27.

[10] *Id*. at P 29.

[11] *Id*. at P 31.

revisions in the Proposed Standard "may not provide adequate electronic access controls for low impact BES Cyber Systems."[12]

The CIP-003-7 electronic access controls provide a flexible, risk-based approach that allows responsible entities to take different approaches to implement controls that allow only necessary inbound and outbound electronic access to low impact BES Cyber Systems for routable communications from Cyber Assets outside the asset containing low impact BES Cyber Systems. Compared to medium and high impact BES Cyber Systems, low impact systems encompass a greater quantity and diversity of assets. Therefore, the ability to implement different electronic access controls is particularly important for low impact BES Cyber Systems, which include a diversity of technologies and implementations for tens of thousands of systems, communication links and networks, and assets across the nation. Flexibility is essential to enable responsible entities—who own and operate these systems—to determine which controls are most appropriate to meet their operational needs and the security objective of allowing only necessary electronic access to low impact BES Cyber Systems.

A prescriptive, one-size-fits-all approach such as the approach used for high and medium impact BES Cyber Systems (CIP-005 and CIP-007) will significantly constrain flexibility while increasing the burden for responsible entities and auditors in documenting and reviewing evidence of compliance without a clear benefit to reliability and security. The burden increases exponentially because the number of BES Cyber Assets contained within low impact BES Cyber Systems far outweighs the number of assets contained within medium and high impact systems.

[12] *Id*. at P 28.

It is also unclear if a more prescriptive approach will have a positive impact to the reliability of the BES.

A risk-based approach is essential to allow responsible entities to focus their resources on the systems that have a higher impact to the BES. Treating the low impact systems like those categorized as medium and high impact is inconsistent with a risk-based approach. By design, low impact BES Cyber Systems are those systems that would have a low impact to the reliability of the BES. In addition, the approach used for high and medium impact BES Cyber Systems use device-level requirements, whereas the low impact BES Cyber Systems are at the facility level due to the sheer number of systems. Using the high and medium impact requirements as a model will diminish the risk-based approach designed into the CIP Reliability Standards and endorsed by the Commission.

In the NOPR, the Commission provides limited discussion on the reliability need, which could justify such a shift away from the risk-based approach that will significantly increase the burdens on responsible entities, beyond the statement that the revisions "may not provide adequate electronic access controls."[13] As a result, the risk to BES reliability is unclear, which would make it difficult for NERC to address the Commission's concerns. Also, until the Section 3 electronic access controls are implemented and audited, it is unclear how the Commission can conclude that there is risk created by the flexibility afforded to responsible entities.

An important consideration is that a more prescriptive approach would likely limit the use of emerging, innovative security approaches for the BES. Flexibility is necessary given the diversity of systems, networks, and assets that for low impact assets. The CIP requirements for

[13] *Id*. at P 28.

medium and high impact BES Cyber Systems has created a more rigid compliance structure. If these requirements become the model for the low impact BES Cyber Systems, this rigid model may discourage responsible entities from implementing emerging and innovative cybersecurity solutions and architectures. For example, virtualization solutions and third-party security providers may bring security benefits, but create compliance risk due to the prescriptive nature of the medium and high impact CIP requirements. The flexible, risk-based approach established by NERC in CIP-003-7 allows responsible entities and auditors to explore such emerging and innovative security controls at a low risk to the reliability of the BES. In addition, a more prescriptive, standardized and rigid model may harm the ability of responsible entities to keep pace with the evolving cybersecurity threat.[14]

The Commission is concerned about affording responsible entities with deference in developing their electronic access controls; however, this "deference" is limited by compliance monitoring and enforcement. During audits, responsible entities must provide specific and sufficient evidence that they are meeting the security objective of permitting only necessary inbound electronic access. It is unclear why the Commission believes this evidence is insufficient for auditors to assess the reasonableness of electronic access controls, especially as CIP-003-7 has not yet been approved by the Commission or implemented by responsible entities. Also, NERC's Compliance Guidance Policy enables the development of Implementation Guidance and CMEP Practice guides that can provide both responsible entities and auditors with a common understanding on how to implement and enforce the requirements.

[14] "The electric industry's reliance on systems and technologies that are commonly available could enable adversaries to develop tools and mechanisms to compromise the most ubiquitous systems." North American Electric Reliability Corporation, *Remote Access Study Report* 5 (2017).

Due to the need for flexibility to control electronic access in low impact BES Cyber Systems, the Trade Associations recommend that the Commission approve the Proposed Standard without modification and monitor its concerns related to deference and inadequate information and electronic access controls. For example, the Commission can direct NERC to conduct a study to assess the implementation by responsible entities of the CIP-003-7 electronic access controls to determine whether there are in fact inadequate controls. A fact-driven assessment would be helpful to inform and demonstrate a reliability and security need for future Commission actions related to the CIP Reliability Standards.

Once the Commission approves a requirement, the implementation plan is triggered for the requirement, which will change again if it is modified by NERC to meet the Commission's proposed directive. Implementation of different versions of a requirement takes time and resources that may not create proportionate benefits to reliability. For many responsible entities, especially those with low impact assets owned by third parties (i.e., shared facilities), physical trips to each asset (i.e., facility), contractual negotiations and expense assignment are required to implement any changes to the sections of CIP-003-7, Attachment 1. Moreover, because assets differ as does the approach responsible entities take to implement the requirements, implementation efforts will vary by asset. These implementation efforts take time and resources—to engage appropriate personnel, assess the configuration at each location, negotiate approaches and expense allocation, implement the changes as necessary and prepare for compliance. One company's estimate is 8 man hours per location, which would take 18 months to complete for all of their assets per version. Resource estimates for smaller complying entities are compounded and more complex. Importantly, such resource sinks most likely will require tradeoffs with other necessary reliability tasks. Therefore, if such resources are employed

multiple times to meet version 6, version 7, and version 8 in short order, the benefit to security or reliability is unclear given these burdens.

If the Commission does not agree and finds that the proposed modification to Section 3 of CIP-003-7 is necessary for reliability, then the Commission should clearly articulate the reliability gap that makes the modification necessary for the reliability of the BES and how this risk to the BES outweighs the burden such a modification would put on responsible entities.

B. The Commission should not direct a modification to the Section 5.2 transient cyber assets managed by a third-party requirement because Section 5 already addresses the Commissions concerns regarding an obligation to address mitigation of malicious code risk.

The Commission proposes to direct NERC to modify the third party managed transient cyber assets requirements in CIP-003-7 to "address the need to mitigate the risk of malicious code."[15] The Commission proposes that because Section 5.2 "does not explicitly require mitigation of the introduction of malicious code from third-party managed Transient Cyber Assets, even if the responsible entity determines that the third-party's policies and procedures are inadequate,"[16] then the "proposed Reliability Standard may, therefore, contain a reliability gap where a responsible entity contracts with a third-party but fails to mitigate potential deficiencies."[17]

Although Section 5.2 does not explicitly require the responsible entity to mitigate the introduction of malicious code, risk mitigation is an explicit obligation under Section 5. For transient cyber assets managed by third-parties, Section 5.2 of Attachment 1 of CIP-007-3

[15] NOPR at P 41.

[16] *Id*. at P 39.

[17] *Id*. at P 40.

requires responsible entities to include in their low impact BES Cyber Asset cybersecurity plan a review of at least one of the third-party's security practices for their transient cyber assets.[18] Section 5 of Attachment 1 of CIP-007-3 requires responsible entities to implement a cybersecurity plan "to achieve the objective of mitigating the risk of the introduction of malicious code to low impact BES Cyber Systems through the use of Transient Cyber Assets."[19] If the responsible entity's plan does not achieve the objective, then the plan will not comply with Section 5.

The standard drafting team's intent of the requirement is made clear in the Supplemental Material for Sections 5 and 5.2, which both require the responsible entities to document how they will mitigate the introduction of malicious code. Specifically, the Supplemental Material for Section 5 states that responsible entities must document and implement a plan "for how they will mitigate the risk of malicious code introduction to low impact BES Cyber Systems from Transient Cyber Assets."[20] The Supplemental Material for Section 5.2 states that responsible entities "are to document and implement their process(es) to mitigate the introduction of malicious code through the use of one or more of the protective measures listed."[21] NERC supports the standard drafting team's intent in their Petition by explaining that the responsible

[18] CIP-003-7, Requirement R2, Attachment 1, Section 5.2 at 23.

[19] CIP-003-7, Requirement R2, Attachment 1, Section 5 at 23.

[20] CIP-003-7 Supplemental Material 50. Although the Supplemental Material does not create binding obligations on responsible entities, the text of the Supplemental Material in the Proposed Standard further clarifies and reinforces that the binding requirements found in CIP-003-7, Attachment 1, Section 5 include the obligation to take additional steps if a third-party's practices do not meet the security objective.

[21] *Id*. at 53.

entity "must take additional steps to meet the stated objective" if the third-party's practices do not meet the security objective.[22]

As a result, the Trade Associations recommend that the Commission approve CIP-003-7 without modification. NERC, the NERC Regional Entities, and the Commission have sufficient record that supports that Part 5.2 of Section 5 of Attachment 1 in CIP-003-7 requires that responsible entities implement measures to mitigate the risk of third-parties introducing malicious code into low impact BES Cyber Systems.

III. CONCLUSION

The Trade Associations appreciate the opportunity to submit comments in response to the NOPR. As discussed herein, the Trade Associations support the proposal to approve the Proposed Standard without modification.

Respectfully submitted,

AMERICAN PUBLIC POWER ASSOCIATION

/s/ Jack Cashin

Delia A. Patterson
Acting Senior Vice President, Advocacy &
Communications and General Counsel
dpatterson@publicpower.org

John E. McCaffrey
Regulatory Counsel
jmccaffrey@publicpower.org

Jack Cashin
Director Policy Analysis and Reliability Standards
jcashin@publicpower.org

[22] NERC Petition at 29.

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

EDISON ELECTRIC INSTITUTE

/s/ Melanie Seader

Mark Gray
Senior Manager, Transmission Operations
mgray@eei.org

Melanie Seader
Associate General Counsel, Reliability and Security
mseader@eei.org

Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

/s/ Randolph Elliott

Randolph Elliott
Senior Director, Regulatory Counsel
randolph.elliott@nreca.coop

Barry Lawson
Senior Director, Regulatory Affairs
barry.lawson@nreca.coop

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818

Dated: December 26, 2017