UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management Reliability Standards	)	**Docket No. RM17-13-000**

COMMENTS OF
THE EDISON ELECTRIC INSTITUTE

I. INTRODUCTION

The Edison Electric Institute ("EEI"), on behalf of our member companies, hereby respectfully submits comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") on January 13, 2018, in the above-referenced docket.[1]

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.

[1] *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044 (2018) ("NOPR").

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. Accordingly, EEI members are directly affected by the NOPR. As discussed herein, EEI encourages the Commission to approve the new Critical Infrastructure Protection ("CIP") Reliability Standard CIP-013-1 (Cyber Security - Supply Chain Risk Management) and new requirements of CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments) and implementation plan without directing further modifications.

II. COMMENTS

The existing CIP Standards take a defense-in-depth approach to cybersecurity for high, medium, and low impact Bulk Electric System ("BES") Cyber Systems and their associated Cyber Assets.[2] The addition of new requirements to CIP-005-6 and CIP-010-3 build upon the existing CIP standards to address vendor remote access and software authentication and integrity risks. However, CIP-013-1 is a new standard that extends CIP cybersecurity requirements from the internal operational environment of Responsible Entity BES to the external procurement of BES Cyber Systems.

In the NOPR, the Commission proposes to approve these new standards but also, reduce the implementation period from the NERC proposed 18 months to 12 months, and direct NERC to modify the proposed requirements to include Electronic Access Control or Monitoring

[2] Associated BES Cyber Assets include Electronic Access Control or Monitoring Systems (EAMCS), Physical Access Control Systems (PACS), and Protected Cyber Assets (PCAs).

Systems ("EACMS") in the applicability of the new requirements. The Commission also proposes to direct NERC to evaluate the supply chain risks posed by Physical Access Control Systems ("PACS") and Protected Cyber Assets ("PCAs") in addition to the study directed by the NERC Board of Trustees ("Board") on low impact BES Cyber Systems, and to file the interim and final study with the Commission.[3]

EEI agrees with the Commission's decision to wait for NERC to study the cybersecurity supply chain risks posed by low impact BES Cyber Systems as well as PACS and PCAs before directing further modifications. However, we believe that it is important to further evaluate potential risks to reliability related to EACMS in this study, before proposing modifications to the CIP Standards. In addition, EEI does not support the Commission's proposal to shorten the implementation period for the new cybersecurity supply chain risk management requirements.

A. The Commission should not shorten the implementation plan because 18 months is needed for Responsible Entities to efficiently and effectively implement the new requirements that require new technology and unprecedented internal and external coordination.

The Commission proposes to shorten the implementation plan for CIP-013-1, CIP-005-6, and CIP-010-3 from 18 months to 12 months because these new requirements are "process-based and do not prescribe technology that might justify an extended implementation period."[4] The Commission believes this shortened implementation period is reasonable and will provide "enhanced security" in a "timelier manner."

EEI believes that the Commission's proposal to shorten the implementation is unreasonable, impractical, and may have unintended consequences. Although the new

[3] NOPR at P 31.

[4] *Id*. at P 44.

requirements for CIP-013-1, CIP-005-6, and CIP-010-3 do not specifically prescribe new technology, EEI believes implementation will require new technologies in addition to new processes in order to comply. Implementation will also require significant and unprecedented internal and external coordination involving legal agreements with entities that are not subject to the Commission's jurisdiction. These entities are not familiar with the Reliability Standards, their intent, and the consequences of non-compliance, and they are not obligated to redress the issues raised by Responsible Entities. Together, these challenges make the Commission's proposal to shorten the implementation period unreasonable.

Implementing the new CIP requirements will require either the procurement of new technology or the revision/expansion of existing technology and close coordination with vendors to implement methods that determine and disable active vendor remote access sessions (CIP-005-6 Requirement R2, Parts 2.4 and 2.5) and to verify the identity of the software source and integrity of the software (CIP-010-3 Requirement R1 Part 1.6). For example, system-to-system access will require new or modified technologies to efficiently and effectively identify and disable remote access. Methods to verify the integrity of software may include the use of encryption, deployment of Public Key Infrastructure (PKI), use of digital signatures, digital fingerprints, and/or technical enforcement of the verification of cryptographic hash values.

Methods to verify the identity of the software source and integrity will also vary by vendor. Some vendors may have an established process or technology for verifications, others may not. Responsible Entities may be able to work with their vendors to develop new tools and processes or they may need to develop their own tools or seek solutions from other vendors.

Responsible Entities must also ensure that all their vendor tools and processes are compatible with their systems, which includes design, implementation, and testing from an operational (e.g., ensuring that such tools and processes meet the security objectives of the new requirements) and compliance perspective. For some vendors, a process-based solution may work, other vendor systems may require new or modified technologies.

Due to variability among vendor products, services, and capabilities, Responsible Entities must coordinate with their vendors to find the most effective and efficient solution to meet the security objectives, which may also change over time as a result of new technology developments, new threats or vulnerabilities, or changes to Responsible Entity systems and policies. As a result, the implementation period proposed by NERC is necessary to enable Responsible Entities to work with their vendors to identify the appropriate technology and process solutions, implement these solutions, test the effectiveness of the solutions, and develop compliance evidence before the compliance effective date of the new requirements.

The new CIP-005 and CIP-010 requirements will apply to all existing medium and high impact BES Cyber Systems, unlike the forward-looking CIP-013 requirements. Existing contracts and agreements may not fully address the currently proposed requirements for vendor remote access and software integrity and authenticity. New contract negotiations may be required to implement the new CIP-005 and CIP-010 requirements for all existing and applicable BES Cyber Systems. Shortening the implementation period, could have the unintended consequence of discouraging the use of more effective and efficient solutions, which may require more time to work out the technical, process, and legal implementation aspects with vendors to meet the CIP-005 and CIP-010 requirements.

The new CIP requirements will require significant internal and external coordination for Responsible Entities. CIP-013 will require complex, cross-functional internal integration of planning, budgeting, information technology, transmission and distribution, supply chain, procurement, and other functions to implement the new CIP Standard. Responsible Entities will also need to coordinate with vendors and service providers to discuss and negotiate how to best address the specific processes required by CIP-013-1 to plan for future BES Cyber System procurements. If the vendors or service providers cannot or will not help Responsible Entities meet their supply chain controls, then Responsible Entities must tailor their plans to the controls that vendors can meet and explore methods to implement other mitigating controls to reduce risk to their systems. Because the compliance obligation is the Responsible Entity's, the identification, acquisition, and implementation of mitigating controls could be very time consuming if this upfront coordination is not done with vendors.

Significant resources will be required due to the volume and complexity of high and medium impact BES Cyber Systems and the volume and diversity of contracts and other agreements for these systems and related services. Also, procurement and deployment cycles often exceed 12 months due to budgeting and resource factors. An implementation period of 18 months would allow more resources to be addressed in yearly budget cycles, which will help to enable contracts under negotiation to meet the new requirements. Without this time, contracts under negotiation may be delayed until resources can be budgeted to meet the new requirements.

Responsible Entities are committed to enhancing security in a timely manner; however, addressing the new supply chain requirements will involve significant coordination by the entities—both internal and external to their organizations—to implement new security and

compliance processes and technology. As a result, the 18 months proposed by NERC is necessary for effective implementation of these supply chain risk management requirements.

B. The Commission should approve CIP-005-6, CIP-010-3, and CIP-013-1 without modification and allow NERC to study the risks related to EACMS.

The Commission proposes to direct NERC to modify the supply chain risk management CIP Reliability Standards (i.e., CIP-005-6, CIP-010-3, and CIP-013-1) to include EACMS.[5] The Commission is concerned since an attacker does not need physical access to compromise a BES Cyber System through an EACMS and an EACMS controls electronic access into an ESP that protects a high or medium impact BES Cyber System and, that an EACMS is the "most likely route" to compromise a BES Cyber System or PCA within an ESP. The Commission concludes that this is "a sufficient basis" to add EACMS to the new supply chain risk management requirements. EEI respectfully disagrees with this conclusion for the reasons discussed below.

First, not every EACMS controls electronic access. An EACMS may simply monitor access and therefore cannot be used to compromise a system within the ESP. As noted by NERC:

> EACMS include a wide variety of devices that perform control or monitoring functions. The risks posed by these various systems may differ substantially. It is important to focus industry resources on higher risk systems. Certain devices that qualify as EACMS may have no or minimal impact on the security of BES Cyber Systems if compromised.[6]

For those systems that control access, EEI agrees with the Commission that if compromised, then such a compromise could "adversely affect the reliable operation of

[5] *Id*. at P 39.

[6] NERC Comments Filed Feb. 26, 2018 under Docket No. RM18-2-000 at 9.

associated BES Cyber Systems."[7] However, as the Commission acknowledges, EACMS are protected under the existing CIP Standards for this very reason.[8] For example, CIP-005-5, Requirement R1, Part 1.3 requires inbound and outbound access permissions and deny by default rules, and Part 1.5 requires detection of known or suspected inbound and outbound malicious communications, both applied at Electronic Access Points that reside on EACMS. CIP-005-5, Requirement 2, Part 2.1, Part 2.2, and Part 2.3 require the use of an EACMS Intermediate System that prevents direct remote access to high and medium impact BES Cyber Systems and PCAs, enforces encryption, and multi-factor authentication for all interactive Remote Access sessions. CIP-007-6, Requirement R1 Ports and Services, Part 1.1 requires enabling only necessary logical network accessible ports for EACMS. Requirement R2's security patch management, Requirement R3's malicious code prevention, Requirement R4's security event monitoring, and Requirement R5's system access control requirements also apply to EACMS. CIP-010-2, Requirement 2, Part 2.1, for EACMS associated with high impact BES Cyber Systems, requires the monitoring, detection, and investigation of unauthorized changes to the baseline configuration of EACMS at least once every 35 days. These EACMS requirements and other applicable CIP requirements are focused on protecting EACMS against compromise. Thus, the mere fact that the security of EACMS is important does not justify a need to modify the proposed supply chain requirements.

Second, the likelihood of compromise from potential supply chain-derived threats to EACMS is not discussed by the Commission in the NOPR and should be evaluated before directing a CIP Standard scope expansion. In the NOPR, statements used to describe potential

[7] NOPR at P 37.

[8] *Id*.at P 36.

risk to EACMS included "may gain control" or "typically become more vulnerable" or "would potentially grant," which are broad and subjective given the layers of defense of the existing CIP Standards, and do not provide a substantive, quantifiable risk from which to impose "objective-based" mandatory reliability standards applicable to EACMS.

The Commission also does not discuss the feasibility of adding EACMS to the supply chain requirements. It would be difficult for an attacker to target the supply chain of an EACMS for BES Cyber Systems because they would have to target all systems that could be used as an EACMS. Many Responsible Entities purchase multiple systems that can be used as an EACMS (e.g., servers, workstations, network switches, routers, firewalls) at the same time for future use. At the time of purchase, Responsible Entities may not know which systems they will be deployed on—non-BES (e.g., a payroll system) or BES. As a result, adding EACMS to the supply chain requirements would require Responsible Entities to expand the CIP supply chain requirements to all purchases of devices that could be used as an EACMS in case they are applied to BES Cyber Systems, or to create entirely new, specific procurement processes for BES Cyber System associated EACMS. The new supply chain requirements specifically excluded EACMS due to these concerns, and these systems are already protected from compromise under the CIP Standards. The reliability or security benefits from adding EACMS to the supply chain requirements are unclear and may have unintended consequences, such as introducing procurement inefficiencies or resource constraints.

Also, an EACMS tends to be commercial, off-the-shelf technology with hardware and software provided by large, dominant commercial vendors that serve a wide variety of business customers outside of the bulk electric system, many of which may not use industrial control systems. In Order No. 829, the Commission directed development of a new or modified standard

to address "supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations,"[9] and the proposed inclusion of EAMCS is a departure from that original scoping. An EACMS and its deployment in roles such as domain controllers, authentication servers, event monitoring systems, or log aggregation systems is not commensurate with the same scoping as an EMS or SCADA industrial control system. As a result, it will be difficult for Responsible Entities to negotiate specific supply chain controls with very large and commercial product and service providers. It is unclear how Responsible Entities can address these issues under the proposed supply chain requirements.

More work is needed to assess whether supply chain risks, related to the various types of an EACMS, necessitate additional modifications to the CIP Standards. Plus, NERC has already begun this work as a part of their Board-directed study. EEI encourages the Commission to wait for this work to be completed to support the record and enable the Commission to make a more informed decision based on the risks to the BES before deciding to add EACMS. Waiting for this work will also allow NERC and Responsible Entities to gain experience implementing the proposed NERC supply chain cybersecurity risk requirements, which will facilitate a more effective and efficient use of Responsible Entity and auditor resources to meet the Commission's security concerns.

C. CONCLUSION

EEI appreciates the opportunity to submit comments in response to the NOPR. EEI recommends that the Commission approve the NERC proposed supply chain risk management

[9] FERC Order No. 829, 156 FERC ¶ 61,050 (Jul 21, 2016).

standards (i.e., CIP-005-6, CIP-010-3, and CIP-013-1) without any modifications, allow 18 months for implementation of the new requirements, and allow NERC to continue its study of the "nature and complexity of cyber security supply chain risks" that will identify potential follow-up actions for Commission review.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

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

Scott I. Aaronson
Vice President, Security & Preparedness

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

Dated: March 26, 2018

Document Content(s)