UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") provides comments on the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking ("NOPR") proposing to approve Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments).[1] NERC supports the Commission's proposal to approve the proposed Reliability Standards. The proposed Reliability Standards are intended to augment the currently-effective Critical Infrastructure Protection ("CIP") Reliability Standards to mitigate cybersecurity risks associated with the supply chain for BES Cyber Systems.[2] As the Commission stated in the NOPR, the proposed Reliability Standards "constitute substantial progress in addressing the supply chain cyber security risks identified by the Commission" in Order No. 829.[3]

In the NOPR, the Commission proposes to direct NERC to:

---

[1] Notice of Proposed Rulemaking, *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044, Docket No. RM17-13-000 (2018).

[2] Unless otherwise designated herein, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf.

[3] *Id*. at P 2.

- Modify the CIP Reliability Standards to include Electronic Access Control and Monitoring Systems ("EACMS") within the scope of the supply chain risk management Reliability Standards.

- Evaluate the cyber security supply chain risks associated with Physical Access Control Systems ("PACS") and Protected Cyber Assets ("PCAs") in the study the NERC Board of Trustees ("Board") requested when it adopted the proposed Reliability Standards.

- File the Board-requested interim and final study reports with the Commission.

The Commission also proposes to reduce the 18-month implementation period set forth in the Implementation Plan associated with the proposed Reliability Standards to 12 months.

As discussed further below, the Commission should refrain from issuing the proposed directive to include EACMS in the proposed Reliability Standards at this time. As NERC stated in its petition, NERC is currently studying, in accordance with the Board's directives to NERC management, whether supply chain risks related to low impact BES Cyber Systems, EACMS, PACS, and PCAs necessitate further consideration for inclusion in a mandatory Reliability Standard.[4] As with low impact BES Cyber Systems, PACS, and PCAs, the Commission should await the results of the Board-requested study to allow for a more comprehensive analysis of the supply chain risks posed by EACMS to determine if and how they should be addressed in each of the proposed Reliability Standards. NERC commits to filing the interim and final study reports with the Commission.

NERC also respectfully requests that the Commission approve the proposed Implementation Plan without modification. As discussed below, the 18-month implementation period provides the proper amount of time to ensure entities can be fully compliant with the proposed Reliability Standards by the effective date.

[4] *Petition of NERC for Approval of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3 Addressing Supply Chain Cybersecurity Risk Management*, at 19-21, Docket No. RM17-13-000 (Sept. 26, 2017).

These comments are organized as follows: Section 1 discusses the Commission's proposed directive related to EACMS and Section 2 discusses the Commission's proposal to reduce the implementation period for the proposed Reliability Standards.

1. The Commission Should Refrain from Issuing the Proposed Directive Regarding EACMS at this Time to Await the Outcome of NERC's Study on Supply Chain Risks and the Scope of the Proposed Reliability Standards

a. Proposed Directive

As noted above, the Commission proposes to direct NERC to: (1) modify the CIP Reliability Standards to include EACMS within the scope of the supply chain risk management Reliability Standards; and (2) evaluate the cyber security supply chain risks of PACS and PCAs in the study requested by the NERC Board. The Commission expressed concern with the exclusion of EACMS, PACS, and PCAs from the scope of the proposed Reliability Standards given the risks they pose due to their location within the Electronic Security Perimeter (i.e., PCAs), or the security control function they perform (i.e., EACMS and PACS).[5]

The Commission identified the need for more immediate action for EACMS (as opposed to PACS and PCAs) on the basis that "EACMS represent the most likely route an attacker would take to access a BES Cyber System or PCA within an [Electronic Security Perimeter]" as their security function is to control electronic access to BES Cyber Systems and PCAs.[6] The Commission noted that PCAs typically become vulnerable to remote compromise once EACMS have been compromised.[7] Further, the Commission noted that, whereas an attacker does not need physical access to the facility housing a BES Cyber System in order to gain access to a BES Cyber

---

5 NOPR at P 34.

6 *Id*. at P 35.

7 *Id*.

System or PCA via an EACMS compromise, accessing a BES Cyber System via a PACS compromise requires physical access.[8]

b. NERC Comments

NERC appreciates the Commission's concern regarding the proposed scope of new Reliability Standard CIP-013-1 and the modifications in CIP-005-6 and CIP-010-3. NERC respectfully requests, however, that the Commission refrain from issuing the proposed directive on EACMS at this time. The Commission has proposed to await the results of the Board-requested study before considering whether low impact BES Cyber Systems, PACS, and PCAs should be addressed in the proposed Reliability Standards. The Commission should similarly await the results of the study with respect to EACMS to allow for a more comprehensive analysis of the supply chain risks for these devices.

In adopting the proposed Reliability Standards, the NERC Board carefully considered the applicability of and requirements in the proposed Reliability Standards. The Board sought to ensure that the proposed Reliability Standards were technically justified and would meaningfully enhance the cyber security posture of the electric industry. The Board adopted the proposed standards as they represented an improvement to the cyber security defenses of applicable entities. For many of the same reasons discussed in the NOPR, however, the NERC Board also acknowledged that further efforts on supply chain management issues were needed to understand and address remaining risks. To that end, the Board issued a series of directives to NERC

[8] *Id*.

management to continue working on supply chain management issues in collaboration with subject matter experts within industry and from other organizations.[9]

Among other things, the Board directed NERC management to conduct a study on the nature and complexity of cyber security supply chain risks, determine whether the proposed Reliability Standards are appropriately scoped to mitigate those risks, and develop recommendations for follow-up actions that would best address any issues identified. The Board directed NERC management to provide an interim report on the study within 12 months and a final report within 18 months. As stated in the Petition, NERC is currently analyzing supply chain risks related to low impact BES Cyber Systems, EACMS, PACS, and PCAs in accordance with the Board's directive to determine whether those Cyber Assets should be included in the proposed Reliability Standard or whether other actions could effectively address the supply chain risks associated with those Cyber Assets.[10]

The study will help determine if and how EACMS should be addressed in the supply chain standards. As defined in the NERC Glossary, the term EACMS encompasses a wide array of systems that perform control or monitoring functions. The risks posed by these various systems may differ substantially. For example, the risks associated with firewalls may be significantly different than the risks associated with a server performing logging and monitoring. A firewall compromise may allow unfettered access to the ESP, whereas a compromise to a logging or monitoring server would provide additional BES Cyber System details. While the system details are valuable and could lead to a compromise, it would typically require additional effort to

---

[9] The Board's directives are available at http://www.nerc.com/gov/bot/Agenda%20highlights%20and%20Mintues%202013/Proposed%20Resolutions%20re%20Supply%20Chain%20Follow-up%20v2.pdf.

[10] Petition at 20-21.

compromise the ESP. As discussed in the Petition, it is important to focus industry resources on higher risk systems.[11] The study will help identify and differentiate the risks presented by the various types of EACMS and inform any future standard development to ensure the scope of the supply chain standards continue to focus industry resources appropriately.

Awaiting the results of the study would also promote a more efficient and effective use of the standards development process and would not result in any significant time delay. The interim study is due to the Board in August 2018 and the final study is due to the Board in February 2019. Allowing for the issues to be studied prior to any standard development work and providing a standard drafting team specific recommendations based on the study would facilitate a more efficient and timely development process. Any changes in the applicability of the proposed Reliability Standards would best be considered by stakeholders at one time. Similarly, consolidating the revisions into one project allows entities to optimize their compliance management processes as it would prevent entities from having to implement two versions of a single standard in close succession.

2. An 18-Month Implementation Period is Appropriate to Ensure Applicable Entities Can Fully Comply on the Effective Date of the Proposed Reliability Standards

In the NOPR, the Commission proposes to reduce the proposed 18-month implementation period to 12 months.[12] The Commission stated that "[t]he 18-month implementation period proposed by NERC does not appear to be justified based on the anticipated effort required to develop and implement a supply chain risk management plan."[13] The Commission noted that "the

---

11 *Id*. at 16-21.

12 NOPR at P 44.

13 *Id*.

security objectives of the proposed Reliability Standards are process-based and do not prescribe technology that might justify an extended implementation period."[14]

NERC respectfully requests that the Commission approve the proposed Implementation Plan without modification. During the development of the proposed Reliability Standards, NERC worked with industry subject matter experts to understand the necessary time for implementing the standards. Those subject matter experts indicated that an 18-month implementation period was needed to afford Responsible Entities sufficient time to develop and implement their supply chain cybersecurity risk management plans according to proposed Reliability Standard CIP-013-1 and implement the new controls required in proposed Reliability Standards CIP-005-6 and CIP-010-3. Although, as the Commission notes, the security objective of proposed Reliability Standard CIP-013-1 is process-based, developing and implementing the requirements in that standard involves performing a complex risk assessment process for planning and procuring BES Cyber Systems. The risk assessment may involve application of risk assessment tools which would need to be procured and installed. The 18-month implementation period allows entities sufficient time to explore these options and implement the CIP-013-1 standard effectively, while also implementing the new requirements in proposed Reliability Standard CIP-005-6 and CIP-010-3.

[14] *Id*.

3. Conclusion

NERC respectfully requests that the Commission consider these comments and approve the proposed Reliability Standards and associated Implementation Plan without modification.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: March 26, 2018