UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management )
Reliability Standards) )

Docket No. RM17-13-000

COMMENTS OF THE MAINE PUBLIC UTILITIES COMMISSION

I. INTRODUCTION

The Federal Energy Regulatory Commission (“Commission”) issued a notice of proposed
rulemaking (“NOPR”) on January 18, 2018, to approve revisions and seek comment for further
revisions to the Critical Infrastructure Protection (“CIP”) Reliability Standards. The Maine
Public Utilities Commission (“MPUC”) provides the following comments on the NOPR.

II. SERVICE AND COMMUNICATIONS

Service in this proceeding should be made upon and communications should be directed
to the following persons:

Lisa Fink, Esq., Counsel for the State of Maine
Public Utilities Commission
101 Second Street
Hallowell, ME 04347
Mailing Address: 18 State House Station
Augusta, ME 04333-0018
(207) 287-1389 (telephone)
lisa.fink@maine.gov

Paul Adamsen
Public Utilities Commission
101 Second Street
Hallowell, ME 04347
Mailing Address: 18 State House Station
Augusta, ME 04333-0018
(207) 287-1397 (telephone)
paul.adamsen@maine.gov
III. BACKGROUND

On July 21, 2016, the Commission issued Order No. 829,1 which directs the North American Electric Reliability Corporation (“NERC”) to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The purpose of the new or modified standard was to “mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.”2 NERC filed proposed reliability standards in response to Order No. 829.3 NERC stated that “the proposed Reliability Standards address the Commission’s directives from Order No. 829 to develop new or modified Reliability Standards that address supply chain cybersecurity risk management for industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (‘BES’) operations.”4 In addition, NERC stated that the proposed reliability standards focus on the following four security objectives: (1) software integrity and authenticity; (2) vendor remote access protections; (3) information system planning; and (4) vendor risk management and procurement controls.”5 NERC further stated that the proposed reliability standards are designed to:

---

1 Order No. 829, Revised Critical Infrastructure Protection Reliability Standards, 156 FERC ¶ 61,050 (2016) (Order No. 829”).
2 Order No. 829, P1.
3 NERC Petition for Approval of Proposed Reliability Standards CIP-013-1, CIP-005-6, and CIP-010-3, Addressing Supply Chain Cybersecurity Risk Management, filed on September 26, 2017, in Docket No. RM17-13-000 (“Petition” or “Proposed Reliability Standard”)
4 Petition at 1.
5 Id at 3.
• Reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.

• Address vendor remote access-related threats, including the threat that vendor credentials could be stolen and used to access a BES Cyber System without the Responsible Entity’s knowledge, as well as the threat that a compromise at a trusted vendor could traverse over an unmonitored connection into a Responsible Entity’s BES Cyber System.

• Address the risk that Responsible Entities could unintentionally plan to procure and install unsecure equipment or software within their information systems, or could unintentionally fail to anticipate security issues that may arise due to their network architecture or during technology and vendor transitions.

• Address the risk that Responsible Entities could enter into contracts with vendors who pose significant risks to their information systems, as well as the risk that products procured by a Responsible Entity fail to meet minimum security criteria.

• Address the risk that a compromised vendor would not provide adequate notice of security events and vulnerabilities, and related incident response to Responsible Entities with whom that vendor is connected.6

NERC proposed that the requirements apply only to the planning and procurement of high and medium impact BES Cyber Systems. In explaining this limitation, NERC stated that it relied on “the existing risk-based framework in the CIP Reliability Standards.” It stated:

Prioritizing high and medium impact BES Cyber Systems in the new supply chain risk management requirements appropriately focuses industry resources on protecting the most impactful BES Cyber Systems. The proposed Reliability Standards prioritize high and medium impact BES cyber systems by specifying mandatory requirements applicable to such systems, while affording entities the flexibility to determine appropriate supply chain cybersecurity risk management steps for low impact BES Cyber Systems. The approach provides an opportunity for industry to address complex supply chain cybersecurity risks in a measured manner, using an established prioritization mechanism. The benefit of this approach is that it allows entities to initially focus their resources on the higher impact BES Cyber Systems, which may eventually lead to better supply chain cybersecurity risk management plans throughout the organization.

. . .

6 Id. at 3–4
During development of the proposed Reliability Standard, entities commented that many of the same vendors supply products and services for all three impact categories and that the same products and services are procured for all three impact categories without differentiation. As such, by requiring that entities implement supply chain cybersecurity risk management plans for high and medium impact BES Cyber Systems, those plans would likely also cover their low impact BES Cyber Systems. Entities may decide not to establish two separate processes for the procurement of products and services for BES Cyber Systems based on impact level, either because during the planning and procurement phase they may not know which environment that system will be placed or simply because it is organizationally more efficient to have a single process for planning and procuring all BES Cyber Systems. Additionally, as Responsible Entities implement their supply chain cybersecurity risk management plans, the vendor community serving the electric industry may respond by including certain security concepts in product design and as standard provisions in future contracts for BES Cyber Systems, regardless of impact level. In this manner, implementation of proposed Reliability Standard CIP-013-1 could enhance the security for all BES Cyber Systems, not just those to which the Reliability Standard specifically applies.\(^7\)

NERC stated that even though the proposed standard does not apply to low-impact cyber assets, it expects that many of these Cyber Assets would be subject to the supply chain risk management plans required by proposed Reliability Standard CIP-013-1. Registered Entities may implement a single process for procuring products and service associated with their operational environments. Further, registered entities may also use the same vendors for procuring PACS, EACMS, and PCAs as they do for high and medium impact BES Cyber Systems such that the same security considerations may be addressed for those Cyber Assets.\(^8\)

In the NOPR responding to the NERC Petition, the Commission stated that “cyber security risks associated with the supply chain for BES Cyber Systems may not be adequately addressed by the NERC proposal.”\(^9\) The NOPR proposes to adopt the proposed Reliability Standards but also proposes that NERC develop modifications to the CIP Reliability Standards to

\(^7\) Id. at 18-19.

\(^8\) Id. at 20.

\(^9\) NOPR at P 31.
include Electronic Access Control and Monitoring Systems (EACMS). In directing NERC to include EACMs in the supply-chain reliability rules, the Commission stated:

EACMS support BES Cyber Systems and are part of the network and security architecture that allow BES Cyber Systems to work as intended by performing electronic access control or electronic access monitoring of the Electronic Security Perimeter (ESP) or BES Cyber Systems.

Since EACMS support and enable BES Cyber System operation, misoperation and unavailability of EACMS that support a given BES Cyber System could also contribute to misoperation of a BES Cyber System or render it unavailable, which could adversely affect bulk electric system reliability. EACMS control electronic access, including interactive remote access, into the ESP that protects high and medium impact BES Cyber Systems. One function of electronic access control is to prevent malware or malicious actors from gaining access to the BES Cyber Systems and PCAs within the ESP. Once an EACMS is compromised, the attacker may gain control of the BES Cyber System or PCA. An attacker does not need physical access to the facility housing a BES Cyber System in order to gain access to a BES Cyber System or PCA via an EACMS compromise.

... In addition, while EACMS is a term unique to NERC-developed Reliability Standards, it is widely recognized that the types of access and monitoring functions that are included within NERC’s definition of EACMS, such as firewalls, are integral to protecting industrial control systems. For example, the Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) identifies firewalls as “the first line of defense within an ICS network environment” that “keep the intruder out while allowing the authorized passage of data necessary to run the organization.” ICS-CERT further explains that firewalls “act as sentinels, or gatekeepers, between zones … [and] [w]hen properly configured, they will only let essential traffic cross security boundaries[,] … [i]f they are not properly configured, they could easily pass unauthorized or malicious users or content.” Accordingly, if EACMS are compromised, that could adversely affect the reliable operation of associated BES Cyber Systems.\footnote{Id. at PP 34-37 (citations omitted).}

IV. COMMENTS

In Order No. 829, the Commission directed NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system
hardware, software, and computing and networking services associated with bulk electric system operations. The purpose of directing the development of this rule was to mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Electric System. The Commission identified supply chain risks including, “the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices.”\textsuperscript{11} The Commission further stated that new types of malware campaigns which have been identified by the Department of Homeland Security are “based on the injection of malware while a product or service remains in the control of the hardware or software vendor, prior to delivery to the customer.”\textsuperscript{12}

The MPUC agrees that a supply chain cybersecurity rule is of critical importance to the reliable operation of the Bulk Electric System. The MPUC further agrees with the Commission that EACMS should be included in the rule. However, many of the concerns addressed by the Commission apply to all classifications of BES Cyber-Systems. The topology of the information system does not necessarily align with the criticality of individual elements of the Bulk Electric System. For this reason, the MPUC urges the Commission to direct that responsible entities apply the proposed requirements to all BES Cyber-System assets, unless the asset in question can be shown to be completely isolated—no direct or indirect connectivity (via wired, radio frequency, infrared, or other interface)—from the BES system. The MPUC also recognizes that supply chain cybersecurity concerns are not limited to BES systems under the Commission’s jurisdiction. Threat vectors will exploit the weakest link. This could include the injection of malware into software or hardware in the distribution systems, over which states have

\textsuperscript{11} Order No. 829, P. 25.
\textsuperscript{12} Id. at P. 26.
jurisdiction, and would likely ultimately affect BES systems. Accordingly, the MPUC urges the Commission to strengthen state-federal partnerships to facilitate the ability of states to address supply chain concerns for assets under state jurisdiction.

Dated: March 22, 2018

Respectfully submitted,

/s/ Lisa Fink

Lisa Fink, Esq.
State of Maine Public Utilities Commission
101 Second Street
Hallowell, ME 04347
Mailing Address: 18 State House Station
Augusta, ME 04333-0018
(207) 287-1389 (telephone)
lisa.fink@maine.gov
CERTIFICATE OF SERVICE

I hereby certify that I have this day served a copy of the foregoing document either by first class mail or electronic service upon each party on the official service list compiled by the Secretary in this proceeding.

Dated at Hallowell, Maine, this 22nd day of March, 2018.

/s/ Lisa Fink

Lisa Fink
State of Maine Public Utilities Commission
101 Second Street
Hallowell, ME 04347
Mailing Address: 18 State House Station
Augusta, ME 04333-0018
(207) 287-1389 (telephone)
lisa.fink@maine.gov