UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management Reliability Standards Revisions	))))	**Docket No. RM24-4**

COMMENTS OF THE ISO/RTO COUNCIL

Pursuant to the Federal Energy Regulatory Commission's ("FERC" or the "Commission") September 19, 2024 Notice of Proposed Rulemaking (NOPR), the ISO/RTO Council ("IRC")[1] hereby submits these comments in the above-captioned proceeding.[2] The NOPR proposes to direct the North American Electric Reliability Corporation (NERC) to develop and submit for Commission approval new or modified Reliability Standards that address the sufficiency of responsible entities' supply chain risk management plans related to the identification of, assessment of, and response to supply chain risks, and the applicability of Reliability Standards' supply chain protections to protected cyber assets. The NOPR states there are increasing opportunities for attacks posed by the global supply chain. In light of the increasing threat environment and the need for improved mitigation strategies, the NOPR states the Commission has identified significant gaps in the provisions of the supply chain risk management Reliability Standards, including gaps related to the: (A) sufficiency of responsible entities' supply chain risk management plans related to the (1) identification of, (2) assessment

[1] The IRC comprises the following independent system operators ("ISOs") and regional transmission organization ("RTOs"): Alberta Electric System Operator ("AESO"); California Independent System Operator Corporation ("CAISO"); Electric Reliability Council of Texas, Inc. ("ERCOT"); the Independent Electricity System Operator ("IESO") of Ontario; ISO New England Inc. ("ISO-NE"); Midcontinent Independent System Operator, Inc. ("MISO"); New York Independent System Operator, Inc. ("NYISO"); PJM Interconnection, L.L.C. ("PJM"); and Southwest Power Pool, Inc. ("SPP"). AESO does not join these comments.

[2] 18 C.F.R. §§ 385.212, 385.213.

of, and (3) response to supply chain risks, and (B) applicability of supply chain risk management Reliability Standards to protected cyber assets. The IRC supports robust supply chain risk management to ensure reliability of the bulk electric system and the ability of responsible entities to identify, assess, and respond to such risks. The IRC offers the following comments on the NOPR.

A. Any Final Rule Directing New Requirements in Supply Chain Risk Management Plans Should Allow for Responsible Entities to Perform Risk Identification.

The NOPR proposes to direct NERC to submit new or modified Reliability Standards to establish specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks[3]. The NOPR would require NERC to establish a maximum time frame between when an entity performs its initial risk assessment during the procurement process and when it installs the equipment. If an entity does not install the equipment or software within the specified time limit, the NOPR states the entity should be required to perform an updated risk assessment prior to installation. The NOPR asks for comments on what factors should inform developing a maximum time frame between the initial risk assessment and a subsequent risk assessment. The NOPR also seeks comment on whether this time frame should vary based on certain factors (e.g., equipment type) and the reasons for any proposed time frame variation.

Any directives to NERC should recognize a responsible entity is best suited to determine how and when to evaluate risk. Neither NERC nor a NERC standards drafting team will fully understand or appreciate each individual responsible entity's unique supply chain risks. Although NERC can develop a requirement that responsible entities identify risks and specify

[3] NOPR at P 32.

the timing requirements for equipment and vendor evaluations, each individual responsible entity is in a better position to understand the risks related to its unique supply chain. Any directive should require NERC to have responsible entities determine in their supply chain risk management plans "the specific timing requirements for a responsible entity to evaluate its equipment and vendors to better identify supply chain risks."

The NOPR proposes to direct NERC to establish requirements for an entity to periodically reassess the risk associated with all supply contracts to identify any supply chain risks that may have developed or changed since the contract commenced.[4] The IRC recommends that responsible entities determine the maximum time frame between risk assessment and contract implementation on a case-by-case basis. Supply chain risk, including the risk associated with the gap between risk assessment and contract implementation, varies depending on the nature of the goods or services being procured and the characteristics of the vendor in question. Some situations may require a very short period between evaluation and implementation (hours or days) and others could be very lengthy (months or years). NERC is not in a good position to evaluate every responsible entity's supply chain risk profile, and this risk would not benefit from a one-size-fits-all mandate. The Commission can direct NERC to develop a requirement that a time frame be established between risk assessment and implementation, but the specific time frame should be established by the responsible entity's supply chain risk management plan and not in a NERC Reliability Standard. Responsible entities need to consider many factors within a supply chain risk management program that will guide the frequency of reassessments. For instance, certain vendors that provide a wide variety of products and services may pose a greater risk to an organization than other vendors. Allowing

[4] NOPR at P 33.

the responsible entity to determine how frequently to assess risk allows the responsible entity to factor in the context of when and how they use each vendor's products and services. In circumstances where it is not practical or feasible to reassess supply chain risk within the timeframe that would ordinarily be required under the responsible entity's risk management program, the responsible entity should also have the flexibility to establish a specific mitigation plan to manage the risk until such time as it can perform a reassessment.

B. The Commission Should Balance the Cost and Scope of any Directive to NERC to Develop Requirements Related to Validation of Completeness and Accuracy of Information Received from Vendors.

The NOPR proposes to direct NERC to submit new or modified Reliability Standards that require a responsible entity to establish steps in its supply chain risk management plan to validate the completeness and accuracy of information received from vendors during the procurement process to better inform the identification and assessment of supply chain risks associated with vendors' software, hardware, or services.[5] The IRC cautions that validation of documentation provided by vendors for the purpose of evaluating supply chain risk is difficult and potentially cost prohibitive. Some well-known approaches to validation of vendor statements regarding supply chain risk involve (a) direct audit of a vendor's practices, (b) third-party audit of a vendor's practices where the third party is hired by the responsible entity, (c) third-party audit of a vendor's practices by a third party hired by the vendor and, (d) attestation by the vendor. In any final rule, the Commission needs to balance the cost of validation with the scope of any directive to NERC to develop requirements related to validation of completeness and accuracy of information received from vendors.

[5] NOPR at P 35.

Direct audit of a vendor's practices can impose significant costs on a responsible entity to hire skilled auditors with subject knowledge of cybersecurity, audit practices, and relevant industry-specific business practices. Engaging a third-party firm to conduct an audit may not cost as much as employing a full-time staff of auditors, but it does create the risk of drastic delays in an entity's procurement process, as there can be significant delays between selection of a vendor and implementation of the contract due to third-party scheduling limitations. It also raises a question of how the entity can properly audit the practices of its selected third-party audit firm.

If a responsible entity requires a vendor to provide the results of a third-party audit conducted by an auditor hired by the vendor, the cost of the vendor's products/services will typically increase as a result, and the responsible entity will typically have less influence, or no influence at all, over the timing, frequency, and quality of the audit, which reduces the overall value of the audit results. Attestation by the vendor may be viable, but only if the vendor is in some way accountable for the accuracy of the attestation and the responsible entity has a contractual right to audit the accuracy of the attestation. For example, a responsible entity might negotiate a contractual obligation that includes some form of financial penalty if the attestation is found to be inaccurate during the duration of the contract. Based on these considerations, any Commission directive that NERC propose a new requirement related to validation that information provided by a vendor is complete and accurate should also direct NERC to provide responsible entities the flexibility to choose the validation approach that best fits the unique circumstances of each contract. This flexibility will assist compliance in the short-term. Any Commission directive to NERC should also encourage and drive further consideration of a longer-term evolution that would take validation responsibilities off of each responsible entity

and allow for the development of third-party verification and other means to more efficiently undertake this important validation task.

C. Any Final Rule Related to a Supply Chain Risk Management Plan Should Recognize Responsible Entities' Own Risk Assessments.

The NOPR proposes to direct NERC to ensure that the new or modified Reliability Standards require that entities establish a process to document, track, and respond to all identified supply chain risks.[6] The NOPR recognizes that a responsible entity can respond to risk in a variety of ways but emphasizes that a responsible entity should document and track its actions. The NOPR indicates that documentation should include what cybersecurity controls are in place or will be put in place to manage the risk while maintaining the overall reliability of the responsible entity's BES Cyber Systems and associated Cyber Assets. The NOPR requests comment on whether and how a standard documentation process could be developed to ensure entities can properly track identified risks and mitigate those risks according to the responsible entity's specific risk assessment. The IRC supports a requirement that responsible entities implement a supply chain risk management plan that includes steps to track identified risks and mitigate those risks according to the entity's specific risk assessment. These steps should align with an industry-accepted risk management framework of the responsible entity's choice. Any directive in a final rule should only seek to establish requirements that responsible entities maintain documentation that addresses certain categories of information and should not attempt to establish a specific document or documents responsible entities must maintain.

---

[6] NOPR at P 38.

D. The IRC Supports the NOPR's Proposal to include Protected Cyber Assets as Applicable Assets under the Supply Chain Risk Management Reliability Standards.

The NOPR proposes to direct NERC to modify the supply chain risk management Reliability Standards to include protected cyber assets as applicable assets.[7] The IRC supports the NOPR's proposal. NERC should modify the supply chain risk management Reliability Standards to include protected cyber assets as applicable assets and to protect them to the same degree as the BES Cyber Systems with which they are associated.

The IRC respectfully requests that the Commission consider these comments in the adoption of any final rule in this proceeding,

Respectfully submitted,

/s/ Margo Caley
Maria Gulluni
Vice President & General Counsel
Margo Caley
Chief Regulatory Compliance Counsel
ISO New England Inc.
One Sullivan Road
Holyoke, Massachusetts 01040
mcaley@iso-ne.com

/s/ Thomas DeVita
Craig Glazer
Vice President-Federal Government Policy
Thomas DeVita
Associate General Counsel
PJM Interconnection, L.L.C.
2750 Monroe Blvd.
Audubon, PA 19403
Phone: (610) 635-3042
Fax: (610) 666-8211
craig.glazer@pjm.com
thomas.devita@pjm.com

/s/ Andrew Ulmer
Roger E. Collanton
General Counsel
Andrew Ulmer
Assistant General Counsel
California Independent System Operator Corporation
250 Outcropping Way
Folsom, California 95630
aulmer@caiso.com

/s/ Raymond Stalter
Robert E. Fernandez
Executive Vice President and General Counsel
Raymond Stalter
Director of Regulatory Affairs
New York Independent System Operator, Inc.
10 Krey Boulevard
Rensselaer, NY 12144
rstalter@nyiso.com

[7] NOPR at P 52.

/s/ Michael Kessler
Michael Kessler
Managing Assistant General Counsel
Midcontinent Independent System Operator, Inc.
720 City Center Drive
Carmel, Indiana 46032
Telephone: (317) 249-5400
Fax: (317) 249-5912
mkessler@misoenergy.org

/s/ Paul Suskie
Paul Suskie
Executive Vice President & General Counsel
Southwest Power Pool, Inc.
201 Worthen Drive
Little Rock, Arkansas 72223-4936
psuskie@spp.org

/s/ Chad V. Seely
Chad V. Seely
Senior Vice President & General Counsel
Nathan Bigbee
Deputy General Counsel
Kennedy R. Meier
Regulatory Counsel
Electric Reliability Council of Texas, Inc.
8000 Metropolis Drive, Bldg. E, Suite 100
Austin, Texas 78744
chad.seely@ercot.com

/s/ Carrie Aloussis
Carrie Aloussis
Senior Manager, Regulatory Affairs
Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto, Ontario M5H 1T1
carrie.aloussis@ieso.ca
Carrie Aloussis@ieso.ca

December 2, 2024

CERTIFICATE OF SERVICE

I hereby certify that I have served the foregoing document upon the parties listed on the official service list in the above-referenced proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Folsom, California, this 2nd day of December 2024.

/s/ Ariana Rebancos

Ariana Rebancos