UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Supply Chain Risk Management	**)**	**Docket No. RM24-4-000**
Reliability Standards Revisions	**)**	
	)	

MOTION TO INTERVENE AND COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION AND THE LARGE PUBLIC POWER COUNCIL

The American Public Power Association ("APPA") and the Large Public Power Council ("LPPC") (together, "Public Power Utilities") hereby move to intervene in this proceeding and comment on the proposals advanced by the Federal Energy Regulatory Commission ("FERC" or "the Commission") in the Notice of Proposed Rulemaking issued in this docket on September 19, 2024 ("NOPR"). APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. Public power utilities are in every state except Hawaii. They collectively serve over 54 million people in 49 states and five U.S. territories, and account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers. LPPC is an association of 29 of the nation's largest municipal and state-owned utilities, representing the larger, asset-owning members of the public power community and approximately 90% of the transmission assets owned by public power. 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 stewardship. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities.

Public Power Utilities here express their general support for the positions taken in comments filed contemporaneously by the Edison Electric Institute ("EEI"). Consistent with

those comments, Public Power Utilities do not oppose FERC's proposal to require the development of a standard to require responsible entities to establish processes to document, track, and respond to identified supply chain risks. NOPR at PP 38-39. Nor do Public Power Utilities object to the proposed extension of supply chain standards to the management of Protected Cyber Assets. NOPR at PP 41-42. Public Power Utilities *do* object to the Commission's proposal to direct NERC to develop revisions to the supply chain standards to require responsible entities "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 risk associated with vendors' software, hardware, or services." NOPR at P 35.

Public Power Utilities are certainly aware of the security risks posed by the equipment and software suppliers upon whom its members must rely on to build, maintain, and manage the Bulk Electric System. Recognizing those risks, Public Power Utilities' members worked on and supported implementation of the suite of supply chain standards addressed in the NOPR. Public Power Utilities particularly supported the CIP-013 requirement calling for responsible entities to develop and implement supply chain risk management plans for high and medium impact BES Cyber Systems. In order the implement and to build upon the standard, Public Power Utilities' members have been actively engaged in questioning and reviewing vendor practices, consistent with guidance and targeted questions recommended by the North American Transmission Forum, in additional to other available resources.[1]

[1] *See: https://www.natf.net/docs/natfnetlibraries/documents/resources/supply-chain/energy-sector-supply-chain-risk-questionnaire.xlsx; See also https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Supply%20Chain%20Risk%20Management%20Guidance.pdf*.

Other programs are available and used by Public Power Utilities' members, including SIG questionnaires (s*ee:* https://www.prevalent.net/blog/standard-information-gathering-sig-questionnaire-explained/#:~:text=What%20is%20SIG%20Lite?,diligence%20than%20higher%2Drisk%20vendors) and the SOC 2 framework (*see https://secureframe.com/blog/soc-2-compliance-checklist*).

Nonetheless, Public Power Utilities' members are acutely aware of their limitations when it comes to their ability to evaluate supplier security practices. In many cases, suppliers are substantially more knowledgeable about the nature of their products and risks (and steps that must be taken to mitigate those risks) than Public Power Utilities' members could reasonably hope to be. In connection with the most sophisticated equipment, there is also the matter of managing the complexity of multiple components of varied origin and the difficulty of tracking custody of the products as they are developed. As to less sophisticated vendors, particularly those with products that are not exclusively used in the electric grid, there is the problem of the vendors' available resources and staffing to field customer inquiries, with the potential result of a meaningfully reduced pool of vendors and shortage of needed equipment and software.

The auditability of steps taken by responsible entities to comply with the proposed new requirement also calls its feasibility into question. Particularly in connection with complex equipment and software, it is not clear what level of documentation and assurance may be called for, or what must be done to validate vendor statements. To be sure, current CIP-013 calls for security risk management plans that require the identification and assessment of cybersecurity risks with due diligence. In proposed requirements to which Public Power Utilities would not object, the NOPR would further require responsible entities to document, track, and respond to identified risks. Yet, Public Power Utilities do not see a way of effectively managing a requirement to validate the completeness and accuracy of vendor representations and documentation.

Nor do Public Power Utilities see that third-party assessors will effectively fill this gap, as the Commission suggests may be an option (NOPR at P 36). While Public Power Utilities' members may well turn to such resources, it is not clear that the requisite expertise exists in the

consulting community, or that value will be added, given the inevitable disclaimers that will be routine regarding reliance on documentation provided. The third-party verification approach will also inevitably add considerable cost to the compliance process.

All of this is not to say that Public Power Utilities do not think that security risk associated with industry vendors is a problem to be ignored. When these issues first came to fore, and in the same time frame in which CIP-013 was being developed, Public Power Utilities urged NERC to take an active role in the development of supplier security protocols, along with a NERC-approved set of protocols for vendors of equipment and software in certain circumstances. That approach still seems to Public Power Utilities to makes sense. And if not NERC, the Department of Energy may play such a role. But in either event, an approach of this nature would recognize the national risk that supplier security practices represents, and the illogic of a decentralized, utility-specific compliance requirement. The proposed approach will, we fear, be costly, inefficient, and ultimately unsuccessful in managing supplier risk.

Respectfully submitted,

American Public Power Association

/s/ Latif M. Nurani
Desmarie M. Waterhouse
Latif M. Nurani
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
Email: dwaterhouse@publicpower.org
lnurani@publicpower.org

Large Public Power Council

/s/ Jonathan Schneider
Jonathan D. Schneider
STINSON LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com