UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

POST WORSKHOP COMMENTS OF THE AMERICAN PUBLIC POWER ASSOCIATION, THE LARGE PUBLIC POWER COUNCIL, AND THE TRANSMISSION ACCESS POLICY STUDY GROUP

The American Public Power Association ("APPA"), Large Public Power Council ("LPPC"), and Transmission Access Policy Study Group ("TAPS") submit these post-workshop comments on the March 20, 2025, Supply Chain Workshop related to 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, LPPC, and TAPS have filed comments on the NOPR.[1]

Our earlier comments share a perspective that is common with other industry trade associations:[2] we do not oppose the NOPR's proposals to require certain responsible entities to document, track, and respond to identified supply chain risks. Nor do we oppose extension of the supply chain standards to Protected Cyber Assets. We do, however, object to the proposed requirement that would require the North American Electric Reliability Corporation ("NERC") to revise its supply chain risk management standards, applicable to high- and medium-impact

[1] Comments of the American Public Power Association and Large Public Power Council, *Supply Chain Risk Management Reliability Standards Revisions*, Docket No. RM24-4-000, eLibrary No. 20241202-5214; Motion for Leave to File Limited Responsive Comments and Limited Responsive Comments of Transmission Access Policy Study Group, *Supply Chain Risk Management Reliability Standards Revisions*, Docket No. RM24-4-000, eLibrary No. 202412-16-5140.

[2] Comments of the Edison Electric Institute, Electric Power Supply Association, and National Rural Electric Cooperative Association, *Supply Chain Risk Management Reliability Standards Revisions*, Docket No. RM24-4-000, eLibrary No. 20241202-5267.

bulk electric system ("BES") cyber systems, to require responsible entities to validate the completeness and accuracy of information received from vendors.

The record developed at the Supply Chain Workshop confirms that the marginal value of a validation requirement does not support the NOPR's proposal to direct revisions to NERC's standards.[3] Workshop panelists explained that the appropriate level of validation of information received from vendors varies significantly based on several factors, including the nature of the product or service, the way in which the utility will use the product or service, and the additional risk management controls the utility incorporates around that product or service. Although responsible entities can and do use a variety of tools to corroborate some of the information received from vendors, much of the information can never be fully validated, so they adopt additional risk mitigation measures to address residual risk associated with vendors' products and services as appropriate.

I. COMMENTS

A. The Workshop's record confirms that the proposed validation requirement is not justified.

The Workshop provided substantial evidence that the NOPR's proposed validation requirement is unjustified. Howard Gugel, NERC's Senior Vice President of Regulatory Oversight, described an appropriate framework for determining whether the validation requirement would be justified. In Mr. Gugel's opinion, the framework must (1) consider the entire suite of risk mitigation, (2) identify any gaps, then (3) determine if a vendor validation requirement significantly addresses the gap. Reflecting on those factors, he commented:

> Given the existing CIP supply chain standard and looking at it with all of the controls that have been placed in the rest of the CIP

[3] Because the official transcript of the Workshop is not yet in the record in this docket, we cite to the Commission's video recording of the Workshop, available at https://www.youtube.com/watch?v=rj8ApZyODiI, with time stamps ("Rec. at hh:mm:ss").

> standards that revolve around vendor access and the requirements around ports and services and those types of things, is there an additional gap that we think is significant enough to reliability that would require this directive that looks at vendor validation or not? That would probably be the question I would step back and say, to quote our CEO, "is the juice worth the squeeze?" Is it worth spending that much time concentrating on that, and does it really get you that much more toward reliability? [4]

We agree with Mr. Gugel's conclusion that the existing suite of reliability standards can address any residual risk left after a utility conducts an appropriate vendor risk assessment.[5] Manny Cancel, CEO of the E-ISAC, also agreed: "We believe the current standards actually do a pretty good job of mitigating these risks, particularly to the BES [Bulk Electric System], and really through the implementation of supply chain security risk management plans."[6]

Other Workshop panelists demonstrated that their utilities use a comprehensive set of risk mitigation techniques *both* at the front-end of procurement by assessing a vendor's risks *and* after procurement to address known and unknown risks. A.J. Jacobs, the Sacramento Municipal Utility District's Chief Information Security Officer, explained that his organization considers third-party certifications as part of a vendor assessment in addition to questionnaire answers, but that not all of the information required by CIP-013 can be validated.[7] Since the risk cannot be completely eliminated through vendor assessment, Mr. Jacobs explained the necessity of managing the residual risk:

> [R]isk is not going to go away. In many cases, what we're thinking about is how we're managing the risk. If we have no validation in what I think the NOPR is getting at, completeness and accuracy of the information, if we have no way to validate, that's considered an

[4] Rec. at 02:29:50.

[5] Rec. at 02:31:01 ("I feel fairly confident that we've got a good suite of standards that will help us manage that control if an entity does an adequate risk assessment that's required in CIP-13.").

[6] Rec. at 00:10:52.

[7] Rec. at 00:51:30 (Third-party certifications "give us some assurance outside of self-attestation that the vendor is doing [what they say they are doing]").

> unknown risk. That means that we have to figure out other means based on our risk posture on how to manage that unknown risk.[8]

Several other panelists emphasized the same concept: vendor assessments can reduce but not eliminate supply chain risks, so utilities employ additional tools to protect their systems.[9]

The Workshop also highlighted several additional tools available for utilities to manage supply chain risks that cannot be addressed through vendor questionnaires. Joe McClelland, Director of FERC's Office of Energy Infrastructure Security, noted actions by the Department of Defense identifying supply chain risks, as well as the Indicators of Compromise ("IOCs") issued nearly daily by the Department of Homeland Security.[10] Mr. Cancel similarly noted information provided regularly by the E-ISAC and NERC on threat information.[11] Panelists confirmed that utilities use that information and take action on it, even when doing so is not required by law.[12]

---

[8] Rec. at 00:56:18.

[9] Rec. at 02:23:40 ("We have this dual mandate of getting the proper equipment and services to serve the customers that are coming our way, we've got to make sure that we've got a secure, safe, reliable, resilient system, and we've got to balance those things. This means we may have to have a piece of equipment on our system that, in the perfect world, we wouldn't deploy. But because we have this environment, we can ramp up monitoring or ramp down monitoring or make other modifications to the way that we approach our business to adjust for it. We have to be doing that because we know our system the best.") (Lance Spross, Oncore); *id.* at 01:45:09 ("attestation in and of itself would not be the complete answer here. It is the full suite of standards and how we comply. It's also the tools that we deploy to detect threats, right? So again, I personally would not just rely on attestation. Certainly, I'd want to have it, but I'd want to make sure my endpoint protection is there, my network monitoring is there, all the tools that we talk about either through our standards or in other discussions, which you all have, are important. So, I think we could also run the risk of fooling ourselves that attestation is a silver bullet here.") (Manny Cancel, NERC); *id.* at 02:27:26 ("it's not like CIP-013 stands alone. We do all the other stuff knowing that probably one of them is not going to be fully vetted...we may fall short on something. That's why there's this defense-in-depth concept, even on the standards. We could spend our entire existence on validating and tracking down all of this information, and I don't know that it would do the grid any good. In the end, we would be leaving something else undone.") (Landon Roeder, NES).

[10] Rec. at 02:49:05.

[11] Rec. at 00:11:30 ("I also want to point out that both NERC and the EISAC continue to monitor and post information regarding supply chain risk. There's a lot of information that goes out almost on a daily basis about the various products, tools, and services that we all utilize.")

[12] *See, e.g.,* Rec. at 02:49:16 (Dart Fee, Entergy).

B. The proposed validation requirement cannot be reasonably managed.

The Workshop provided substantial evidence that the NOPR's proposed requirement for responsible entities to validate information received from suppliers would be unduly costly and unmanageable. Mr. Cancel, for NERC, acknowledged how challenging it can be to validate vendor-supplied responses "due to the sheer volume of information."[13]

Large and small utilities all report challenges associated with validating vendor-supplied information or imposing contractual provisions on vendors. Landon Roeder, of Nashville Electric System, stated it plainly: "We have limited negotiating power. Our entity can't really go push anybody around…our legal and political clout is very limited when it comes to the procurement process."[14] Dart Fee, of Entergy, confirmed that even large utilities experience limited negotiating power with organizations that provide technology products and service to the electric industry: "when we get to that negotiating table, we feel the pressure to simply sign their paper as well, as the saying goes."[15]

Panelists acknowledged the existence and value of third-party certifications and secondary sources that can be used to corroborate some vendor information. But panelists also described the limitations of these tools: no certification body nor any secondary source can comprehensively validate all the information required by CIP-013,[16] and the cost of conducting

[13] Rec. at 00:14:11 ("Companies can be challenged to validate the completeness and accuracy of information collected by vendors due to the sheer volume of information. In addition, companies are often challenged by vendors who either respond poorly or are unwilling to respond to the questions, making it difficult to validate the completeness and accuracy of the information collected.") (Manny Cancel, NERC)

[14] Rec. at 02:07:47; *see also id.* at 00:22:03 ("The most sophisticated equipment and software we purchase is highly complex and has components of varied origin. It is not reasonable to expect that we will be able to adequately verify representations made regarding the security of the vendors.") (AJ Jacobs, SMUD).

[15] Rec. at 02:09:37; *see also id.* at 02:12:03 ("We're not completely at their mercy, but they're not really interested in having a big conversation about adding additional things onto their plate to do just so they can serve our needs.") (Lance Spross, Oncor).

[16] Rec. at 00:57:37 ("at times there's a robust marketplace for third-party validation at a price point that works, and you can be confident that that third-party validator is going to add value. At other times, depending on a number of factors, there just isn't that supply of third-party validation.") (Laura Schepis, NEMA); *id.* at 03:03:42 ("there are no

substantial review of secondary sources to corroborate vendor information is not warranted for all systems.[17]

Echoing comments made by Mr. Cancel, Bob Kolasky, CEO of Exiger, explained the huge complexity facing any utility seeking individually to conduct validation of potential suppliers:

> Supply chains have expanded and vendors have diversified. This means that major utilities could literally have thousands of vendors who can introduce potential risk into their operations. Because of that, that number demands a criticality approach to triage the vendors who hold most of the risk. So, there has to be risk assessment before you decide how to dive deeper into assessments and validation. It also may call for product assurance approaches for the most important products, which can't be accomplished merely via surveys. [18]

Given the complexity of the supply chain, Mr. Kolasky concluded that imposing a validation requirement on individual utilities "at one point of the risk mitigation or risk assessment process [is] going to leave other risks and give you a false sense of comfort."[19]

C. The highly varied nature of supplier risk does not lend itself to a uniform standard.

A common refrain throughout the entire Workshop is that "one size doesn't fit all" when it comes to vendor assessment.[20] The appropriate level of vendor assessment—and validation of information—varies significantly based on several factors, including the nature of the product or

single certifications that meet all of the requirements of CIP 13, but they do help, and they do give us a sense of validation and reduce risk of that company.") (Landon Roeder, NES).

[17] Rec. at 02:22:33 ("So for me to give [low-risk vendors] a huge requirement to go fill out a big form and to go through all sorts of third-party validations and certifications, not only is it a waste for them, but it's a waste for me. On the other hand, there are other products and services and systems that I need to really focus more of my time on and do a thorough risk evaluation and then come back and say, 'Alright, these are the people I need to focus more on.'") (Landon Roeder, NES).

[18] Rec. at 00:29:44.

[19] Rec. at 00:46:43.

[20] *See, e.g.*, Rec. at 00:59:30 (Alan Hurt summarizing Panel One's main takeaways as "One, there's no one-size-fits-all, and two, risk is a main driver here, whether that be through your own assessment or from an inherent risk assessment.").

service, the way in which the utility will use the product or service, and the additional risk management controls the utility incorporates around that product or service.

The NOPR characterized inconsistency in vendor assessment as a potential gap in the existing reliability standards.[21] But NERC's Howard Gugel explained why that isn't the case: "I don't believe that inconsistent application is a gap. If you look at an entity's size, their exposure, their risk to the bulk electric system, they probably can have inconsistent application of their risk analysis and still provide an adequate view of what the risk of the vendor is and what their risk is to the bulk electric system."[22]

Furthermore, given the varying nature of supply chain risks, Mr. Gugel expressed his concern about drafting appropriate and enforceable language in a reliability standard: "I think about how difficult it's going to be to come up with language in the supply chain standard that would meet the needs of a large investor-owned utility and a small municipal in a rural setting, which has maybe 10 or 11 employees total dedicated to their electric service."[23]

D. The Workshop's record supports a renewed effort to address supplier risks centrally.

The value of federal government support for vendor assessment was one of three main themes that Director McClelland took from the Workshop's second panel:

> It would be helpful if there was some sort of a certification process and certainly information flow from the federal government, maybe in addition to the IOCs. There's information that's released about supply chains, vulnerabilities associated with it, even vendors. It would be helpful where the federal government could take the lead and industry itself, perhaps you'd be willing to pay a premium if the industry would sort of self-certify or certify through, we'll just say, a national lab, something or other like that. So, that may be

[21] NOPR, P 27.

[22] Rec. at 03:17:45.

[23] Rec. at 02:15:14.

> something that you'd be interested in, and should it be good for America? I mean, that's just the right thing to do. [24]

We urge the Commission to take up the call, advocated in our initial comments, to coordinate federal government efforts in this area. Whether the approach involves the creation of a "safe list" of vendors, a "blacklist" of vendors or products to avoid, or other mechanisms such as improved IOCs, there is clearly an opportunity for the federal government to do more to improve electric industry supply chain risk mitigation. The record in this proceeding is clear that relying on a utility-by-utility approach to vendor risk assessment is neither efficient nor effective.

II. CONCLUSION

Based on the record developed in this proceeding, including evidence from the Workshop, APPA, LPPC, and TAPS urge the Commission not to adopt the proposed directive to require NERC to revise its supply chain risk management standards to require responsible entities to validate the completeness and accuracy of information received from vendors.

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

[24] Rec. at 03:00:58.

Transmission Access Policy Study Group
/s/ Cynthia S. Bogorad
Cynthia S. Bogorad
Lauren L. Springett
SPIEGEL & MCDIARMID LLP
1818 N Street, NW
Washington, DC 20036
(202) 879-4000
cynthia.bogarad@spiegelmcd.com
lauren.springett@spiegelmcd.com