UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF AMERICAN PUBLIC POWER ASSOCIATION, ELECTRICITY CONSUMERS RESOURCE COUNCIL, LARGE PUBLIC POWER COUNCIL, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND TRANSMISSION ACCESS POLICY STUDY GROUP

The American Public Power Association ("APPA"), the Electricity Consumers Resource Council ("ELCON"), the Large Public Power Council ("LPPC"), the National Rural Electric Cooperative Association ("NRECA"), and the Transmission Access Policy Study Group ("TAPS") (collectively, "Joint Trade Associations") submit these comments in response to the Federal Energy Regulatory Commission's ("Commission" or "FERC") January 18, 2018 Notice of Proposed Rulemaking in the above-captioned docket.[1]

I. INTRODUCTION AND SUMMARY

The Commission proposes to approve supply chain risk management Reliability Standards submitted by the North American Electric Reliability Corporation ("NERC") in response to a directive in Commission Order No. 829.[2] While the Commission finds that NERC's proposed Reliability Standards "constitute substantial progress in

[1] *Supply Chain Risk Management Reliability Standards*, 162 FERC ¶ 61,044 (2018), 83 Fed. Reg. 3433 (Jan. 25, 2018) ("NOPR").

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016). Specifically, the Commission proposes to approve new Reliability Standard CIP-013-1 (Cyber Security – Supply Chain Risk Management) and revisions to Reliability Standards CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)) and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). The Commission also proposes to approve the violation risk factors and violation severity levels associated with the proposed Reliability Standards. *See* NOPR at P 3.

addressing the supply chain cyber security risks identified in Order No. 829,"[3] the NOPR also includes a proposed directive requiring NERC to develop modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards to include Electronic Access Control and Monitoring Systems ("EACMS") associated with medium and high impact Bulk Electric System ("BES") Cyber Systems within the scope of the supply chain risk management Reliability Standards.[4] The Commission further proposes to direct NERC to evaluate the cyber security supply chain risks presented by Physical Access Control Systems ("PACS") and Protected Cyber Assets ("PCAs") in the study of cyber security supply chain risks that was requested by the NERC Board of Trustees ("BOT") in its resolutions of August 10, 2017.[5] Finally, the Commission proposes a 12-month implementation period in lieu of the 18-month period proposed by NERC.[6]

Joint Trade Associations support Commission approval of NERC's proposed supply chain risk management Reliability Standards. The proposed standards fulfill Order No. 829's directive and would mitigate supply chain cyber security risks to the BES while appropriately focusing on the systems and assets that are most critical to reliable operation of the BES.

Joint Trade Associations urge the Commission to refrain from issuing a directive requiring NERC to include EACMS within the scope of the CIP Reliability Standards at

---

[3] NOPR at P 30.

[4] *See* NOPR at PP 4, 33-39. Reliability Standard CIP-002-5.1a (Cyber Security System Categorization) provides a "tiered" approach to cyber security requirements, based on classifications of high, medium and low impact BES Cyber Systems.

[5] NOPR at PP 4, 40-43. The Commission proposes to direct NERC to file the BOT-requested study's interim and final reports with the Commission upon their completion. NOPR at P 4, 43.

[6] *Id.* at P 44. As proposed by the Commission, the Reliability Standards would "become effective the first day of the first calendar quarter that is 12 months following the effective date of a Commission order approving the Reliability Standards." *Id.*

this time. Instead, the Commission should await the results of the BOT-requested study on cyber security supply chain risks, as NERC suggests in its NOPR comments, consistent with the Commission's proposed approach for PACS and PCAs. While Joint Trade Associations appreciate the Commission's desire to ensure that the supply chain Reliability Standards do not reflect gaps that could put BES Cyber Systems at risk, a blanket requirement to include EACMS could significantly increase the compliance obligations placed on Responsible Entities without any commensurate reliability benefit. Refraining from issuing a directive to include EACMS at this time would promote a more efficient and effective standards development process for any BES Cyber Assets that NERC or the Commission determine should be included within the scope of the supply chain Reliability Standards.

The Commission should also reconsider its proposal to require a 12-month implementation period instead of the 18-month period proposed by NERC. Joint Trade Associations respectfully disagree with the Commission's suggestion that the proposed Reliability Standards could be implemented in 12 months because they are "process-based."[7] Implementing the new and revised standards will require new technology as well as process enhancements. Complying with the requirements will also necessarily require a considerable amount of coordination with third-party vendors. A reasonable timeline for accomplishing these necessary tasks exceeds 12 months, and accordingly, Joint Trade Associations submit that 18 months is an appropriate amount of time for Responsible Entities to efficiently and effectively implement the new requirements.

[7] NOPR at P 44.

II. INTERESTS OF JOINT TRADE ASSOCIATIONS

APPA is the national service organization representing the interests of the nation's 2,000 not-for-profit, community-owned electric utilities. Public power utilities account for 15% of all sales of electric energy (kilowatt-hours) to ultimate customers and collectively serve over 49 million people in every state except Hawaii. Approximately 261 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout the United States. Many ELCON members also operate behind-the-meter generation and are NERC registered entities, and ELCON has actively participated in NERC's stakeholder and standards development processes. Reliable electricity supply is essential to its members' operations.

LPPC is an association of the 26 largest state-owned and municipal utilities in the nation and represents the larger, asset-owning members of the public power sector.[8] LPPC members are also members of APPA and own approximately 90% of the transmission assets owned by non-federal public power entities. LPPC members are

[8] LPPC's members are: Austin Energy, Chelan County Public Utility District No. 1, Clark Public Utilities, Colorado Springs Utilities, CPS Energy (San Antonio), ElectriCities of North Carolina, Grand River Dam Authority, Grant County Public Utility District, IID Energy (Imperial Irrigation District), JEA (Jacksonville, FL), Long Island Power Authority, Los Angeles Department of Water and Power, Lower Colorado River Authority, MEAG Power, Nebraska Public Power District, New York Power Authority, Omaha Public Power District, Orlando Utilities Commission, Platte River Power Authority, Puerto Rico Electric Power Authority, Sacramento Municipal Utility District, Salt River Project, Santee Cooper, Seattle City Light, Snohomish County Public Utility District No. 1, and Tacoma Public Utilities.

located throughout the nation, both within and outside RTO boundaries, and they are subject to the Commission's electric reliability regulations and requirements as set forth in Federal Power Act Section 215.

NRECA represents the interests of the nation's more than 900 rural electric utilities responsible for keeping the lights on for more than 42 million people across 47 states. Electric cooperatives are driven by their purpose to power communities and empower their members to improve their quality of life. Affordable electricity is the lifeblood of the American economy, and for 75 years electric co-ops have been proud to keep the lights on. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve. Additionally, NRECA's members participate in all of the organized wholesale electricity markets throughout the country. And for this reason, NRECA participates in a variety of Commission proceedings, rulemakings and notices of inquiries on behalf of its members affecting the reliability of the BES.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[9] TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the Bulk Power System and are highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC reliability standards.

[9] David Geschwind, Southern Minnesota Municipal Power Agency, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

Communications regarding these proceedings should be directed to the individuals listed in Attachment A.

III. COMMENTS

A. Joint Trade Associations Support Approval of the Supply Chain Reliability Standards Proposed by NERC

Addressing supply chain risk is an important objective in protecting the reliability of the BES, and Joint Trade Associations support the supply chain Reliability Standards as proposed by NERC in its September 26, 2017 petition ("NERC Petition"). While Joint Trade Associations have previously expressed reservations about adopting mandatory supply chain CIP Reliability Standards, Joint Trade Associations believe that NERC's proposed standards fulfill Order No. 829's directive while appropriately focusing on the systems and assets that are most critical to reliable operation of the BES. Further, Joint Trade Associations do not oppose the Commission directing that NERC evaluate the cyber security supply chain risks presented by PACS and PCAs in the BOT-requested study, as proposed in the NOPR.

Consistent with NERC's risk-based approach to CIP standards, the NOPR proposes that the supply chain standards would apply only to medium and high impact BES Cyber Systems.[10] In its Petition, NERC explained that excluding low impact BES Cyber Systems will focus industry resources on protecting those systems with heightened risk, while not being overly burdensome or diverting resources to protecting lower risk assets.[11] Joint Trade Associations strongly support this conclusion, and appreciate the Commission's proposal to limit the applicability of the proposed Reliability Standards to

[10] *See* NOPR at P 33.

[11] *See* NERC Petition at 18-19.

medium and high impact BES Cyber Systems, as well as its decision to assess the results of the BOT-requested study "before considering whether low impact BES Cyber Systems should be addressed in the supply chain risk management Reliability Standards."[12]

Among the concerns previously expressed by Joint Trade Associations about supply chain reliability standards is that supplier practices are generally not within the direct control of registered entities, and that compliance with too prescriptive a requirement could necessitate utilities involving themselves intimately in vendor processes they do not have the expertise or manpower to supervise. These vendors are not subject to direct FERC oversight, and for this reason Joint Trade Associations emphasize that federal authorities other than FERC may have a role to play in helping protect critical infrastructure. Joint Trade Associations urge FERC to work with the industry and other relevant federal authorities in order to address these security issues holistically.

As to the course of action the Commission and NERC have chosen to take, Joint Trade Associations appreciate that NERC's proposed supply chain Reliability Standards address these challenges by permitting Registered Entities to undertake a variety of approaches designed to address procurement risks, investing them with discretion in dealing with vendors. The proposed standards are flexible and risk-based, enabling utilities to make informed judgments regarding the risk that upstream assets pose to the BES when incorporated into grid operations. Further, the standards do not require active management by utilities of third-party processes, nor hold utilities liable for vendor errors.

[12] NOPR at P 33.

Joint Trade Associations recognize that compliance in this area will involve the evolution of best practices. Among the emerging practices Joint Trade Associations members anticipate promoting will be the standardization of protocols adopted by vendors in order to represent that they have met specified security objectives and protocols. That approach will appropriately place on the vending community the responsibility for security practices, while engendering confidence in the purchasing community that vendors' products and communications/operations are secure. Joint Trade Associations anticipate that movement in this direction may be facilitated through coordination between the industry, the Commission, and potentially others within the federal government.

B. The Commission Should Not Direct NERC to Include EACMS in the Supply Chain Reliability Standards

Although Joint Trade Associations support the Commission's proposal to approve the supply chain Reliability Standards submitted by NERC, Joint Trade Associations urge the Commission to reconsider its proposal to issue a directive requiring NERC to include EACMS associated with medium and high impact BES Cyber Systems within the scope of the Reliability Standards. The better course would be to adopt the suggestion in NERC's NOPR comments to await the outcome of the BOT-requested study that will evaluate whether supply chain risks related to EACMS require further consideration for inclusion in a mandatory Reliability Standard.[13] Allowing the BOT-requested study process to be completed (as the Commission proposes with respect to PACS and PCAs) would be a more efficient and effective way to promote meaningful mitigation of cyber

[13] *See* NOPR at P 41, n.42 (citing NERC Petition at 21).

security supply chain risks than an immediate, blanket requirement to include EACMS within the standards.

The Commission's concern about EACMS appears to be based, to a large degree, on its understanding that "EACMS control electronic access, including interactive remote access, into the ESP that protects high and medium impact BES Cyber Systems."[14] The Commission suggests that "[o]nce an EACMS is compromised, the attacker may gain control of the BES Cyber System or PCA,"[15] and, thus, "EACMS represent the most likely route an attacker would take to access a BES Cyber System or PCA within an ESP."[16]

The EACMs currently in use by Responsible Entities comprise a variety of assets that perform diverse control or monitoring functions. Due to the diversity of EACMS and their functions, their potential BES reliability risk may vary greatly. As the name indicates, some EACMS merely perform a monitoring function, and do not, as the NOPR suggests, control access to the Electronic Security Perimeter ("ESP") and/or BES Cyber Systems. NERC's NOPR comments, for example, draw a contrast between a firewall that may control access to an ESP, with a server that simply performs a logging and monitoring function. Although these assets are both classified as EACMS, NERC explains, only the firewall, if compromised, could potentially allow unauthorized access to the ESP.

---

[14] *Id.* at P 35.

[15] *Id.*

[16] *Id.*

The BOT-requested study is likely to provide more specific information and analysis concerning whether any category of EACMS might be appropriately included within the scope of the supply chain Reliability Standards. To the extent that it may be reasonable to include certain EACMS (or PACS, or PCAs) within the scope of the supply chain Reliability Standards to address the concerns cited by the Commission, the results of the BOT-requested study will provide a more fully-informed basis for that decision. This approach, moreover, would be consistent with NERC's risk-based approach to CIP standards. In contrast, a potentially unnecessary or overbroad blanket direction to include all EACMS, regardless of function or risk, within the scope of the Reliability Standards could have an adverse impact on cyber security by requiring Responsible Entities to devote compliance resources to assets that present no significant BES reliability threat.

Refraining from issuing a directive to include EACMS at this time would also promote a more efficient and effective standards development process. The BOT-requested study will further assess supply chain risks to evaluate whether the proposed Reliability Standards are appropriately scoped, including with respect to the treatment of EACMS, PACS and PCAs.[17] As NERC explains in its comments, the BOT-requested study should identify whether actions other than mandatory standards could effectively address supply chain risk associated with EACMS and other Cyber Assets. Allowing EACMS to remain a subject of the study process is likely to result in a more complete and thorough analysis of the supply chain risks associated with Cyber Assets. To the extent that the BOT-requested analyses prompt additional changes to the Reliability Standards (either from NERC or as directed by the Commission), it would be more

[17] *See* NERC Petition at 20-21.

efficient to have these matters, and any other related outstanding issues, addressed by a single drafting team, rather than have a drafting team responding to a directive to include EACMS and a second drafting team modifying the standards per the BOT-requested study.[18] Joint Trade Associations encourage the Commission to avoid issuing directives that necessitate constant and overlapping CIP standard revisions and resulting complex implementation plans.

From a broader perspective, Joint Trade Associations view the CIP standards as providing a cyber security framework that establishes an internal process that allows entities to quickly adapt to the evolving threat landscape. Mandatory standards, by their nature, cannot easily adapt to dynamic problems like cyber security threats, which operate within the backdrop of rapidly changing technology. Joint Trade Associations believe that in many instances imposing specific solutions for specific threats or vulnerabilities in the form of mandatory standards can slow innovative approaches to cyber security among electric utilities. NERC, industry, and the Commission have other tools, programs, and best practices they can use to meet evolving cyber security supply chain risk. Indeed, the BOT-requested study process is likely to more clearly identify best practices in supply chain risk management.[19] Utilities can also address security threats in the context of BES reliability with appropriate access to classified threat data and close collaboration with federal agencies and industry peers, such as through the

[18] There is a significant overlap among the cyber security and infrastructure CIP standards under development at NERC and the subject matter experts ("SMEs") working on them. Efficiently leveraging these SMEs will require giving them the benefit of all the current EACMS research, as well as the Commission's assessment of that research, prior to their addressing EACMS for risk-based standard development.

[19] *See* NERC Petition at 35-36.

Electricity Subsector Coordinating Council and NERC's Electricity Information Sharing and Analysis Center ("E-ISAC"). NERC also has a formal Alert process that can quickly provide critical information and recommended actions related to any incident or threat.

Joint Trade Associations would also note that opportunities to engage vendors on supply chain security issues can best occur outside of a compliance environment. For example, APPA is party to a cooperative agreement with the U.S. Department of Energy ("DOE") that will, among other things, produce a cyber security self-assessment tool for public power utilities, including a module relating to supply chain risk. In addition, the NERC BOT effort has industry and vendors addressing both contracting best practices and development of potential vendor verification. In that context, Joint Trade Associations would note that before mandatory CIP standards were prescribed for the electric industry, DOE had published its Electric Sector Cyber Security Capability Maturity Model ("C2M2"), an aspirational voluntary framework. Joint Trade Associations believe that the innovative efforts being explored, such as vendor verification, can best succeed without the influence of potential compliance obligations from standards requirements.

C. The Commission Should Not Shorten the Implementation Period to 12 Months

The Commission proposes to direct NERC to shorten the implementation period for CIP-013-1, CIP-005-6, and CIP-010-3 from 18 months to 12 months because these new requirements are "process-based and do not prescribe technology that might justify an extended implementation period."[20] While the Commission is correct that the

[20] NOPR at P 44.

proposed Reliability Standards focus on implementing processes to guard against cyber security supply chain risks, the standards' requirements will also require new technology enhancements. For example, complying with new CIP-005-6 will require coordination with vendors to implement methods to determine and disable active vendor remote access sessions. In addition to warranty and contract review, initial discussions with vendors suggest that technology upgrades will be necessary. The new CIP-010-3 requirements to verify the identity of the software source and integrity of the software will also require implementing new technology such as performing cryptographic hash functions to fingerprint files and mapping them to appropriate software products. These technologies will have to be purchased, and it will take time to ensure their appropriate implementation.

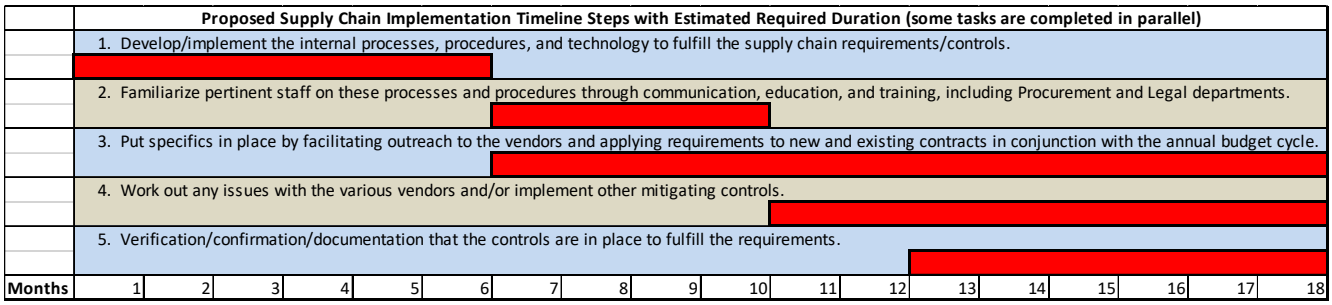
Implementing the proposed supply chain Reliability Standards will require utilities and their vendors to work together to provide appropriate solutions, and that coordination will take time. Utilities will need to coordinate with vendors and service providers to negotiate how to address the specific processes required by CIP-013-1 used in procuring BES Cyber Systems. Utilities anticipate that the result of such discussions will suggest that registered entities will need to implement other mitigating controls to reduce risk to their systems.

Managing supply chain risk also requires coordination of several utility areas such as operational planning, legal, procurement, and information technology. In particular, the increased involvement of utility supply chain personnel in CIP compliance activities will require lead time for the relevant personnel to develop a more detailed understanding

of the CIP program, terminology, and standards, in order to effectively incorporate CIP compliance into their function.

Should the proposed standards impact significant high and medium BES Cyber Systems in a way that requires technology changes, such changes will be included in a utility's long-term capital budgets. Such decisions typically require board-level corporate review and would need to be incorporated into the annual budgeting cycle. Therefore, an implementation period of 18 months would facilitate a more efficient and effective implementation.

Joint Trade Associations, in consultation with members that would be subject to the supply chain Reliability Standards, developed the compliance timeline below which illustrates the reasonableness of an 18-month implementation period. The key point emphasized by members focusing on anticipated compliance, and underscored by the timeline, is that certain activities in the critical path to compliance will be undertaken sequentially. The development of needed internal processes must precede staff training, which is in turn, a predicate for work with vendors.



For these reasons, Joint Trade Associations believe the implementation of the Supply Chain standards will require the 18-month period proposed in the NERC Petition.

IV. CONCLUSION

For the reasons discussed above, the Commission should: (i) approve the supply chain Reliability Standards as submitted by NERC; (ii) refrain from issuing a directive requiring NERC to include EACMS within the scope of the CIP Reliability Standards; and (iii) approve NERC's proposed 18-month implementation period instead of the 12-month period proposed in the NOPR.

[Signature block appears on the next page]

Respectfully submitted,

/s/ John E. McCaffrey
John E. McCaffrey
Regulatory Counsel
Jack Cashin
Director of Policy Analysis & Reliability Standards
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

American Public Power Association

/s/ Randolph Elliott
Randolph Elliott
Senior Director, Regulatory Counsel
Barry Lawson
Senior Director, Regulatory Affairs
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818

National Rural Electric Cooperative Association

/s/ John P. Hughes
John P. Hughes, President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390

Electricity Consumers Resource Council

/s/ Cynthia S. Bogorad
Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000

Transmission Access Policy Study Group

/s/ Jonathan D. Schneider
Jonathan D. Schneider
Jonathan P. Trotta
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue, NW
Suite 800
Washington, DC 20006
(202) 728-3034

Large Public Power Council

ATTACHMENT A

LIST OF PERSONS TO RECEIVE COMMUNICATIONS

For APPA
John E. McCaffrey
Regulatory Counsel
Jack Cashin
Director of Policy Analysis & Reliability Standards
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900
jmccaffrey@publicpower.org
jcashin@publicpower.org

For ELCON
John P. Hughes
President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
(202) 682-1390
jhughes@elcon.org

For LPPC
Jonathan D. Schneider
Jonathan P. Trotta
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

For NRECA
Randolph Elliott
Senior Director, Regulatory Counsel
Barry Lawson
Senior Director, Regulatory Affairs
NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818
randolph.elliott@nreca.coop
barry.lawson@nreca.coop

For TAPS
Cynthia S. Bogorad
Latif M. Nurani
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

John Twitty
Executive Director
TRANSMISSION ACCESS POLICY STUDY GROUP
PO Box 14364
Springfield, MO 65814
(417) 838-8576
jtwitty@tapsgroup.org