UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards	**)** **)**	**Docket No. RM15-14-000**

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

I. Introduction

The American Public Power Association ("APPA"), Large Public Power Council ("LPPC"), and the Transmission Access Policy Study Group ("TAPS") (collectively, "APPA, *et al*.") provide these supplemental comments in response to the proposal advanced in the Commission's Notice of Proposed Rulemaking ("NOPR") in this docket directing NERC to develop new or modified reliability standards that would "provide security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations."[1] The comments respond to discussion at the Commission's related January 28, 2016 technical conference. APPA, *et al*. recognize that the Commission has not called for supplemental comments, but ask that they be considered as a further reflection on the Commission's proposal, in view of the discussion at the technical conference.

APPA, *et al*. joined the industry trade association comments filed in this docket on September 21, 2015.[2] Those comments generally supported the NOPR, but opposed the

[1] *Revised Critical Infrastructure Protection Reliability Standards*, 152 FERC ¶ 61,054 at P 66 (2015).

[2] *See* Comments of the Edison Electric Institute, the American Public Power Association, National Rural Electric Cooperative Association, Electric Power Supply Association, Electricity Consumers Resource Council, Transmission Access Policy Study Group, and the Large Public Power Council, Docket No. RM15-14-000 (filed Sept. 21, 2015), at pp. 15-27.

proposed supply chain directive. While APPA, *et al*. continue to share the concerns articulated in those initial comments, here we provide further input regarding the nature of potential standards in this area that may help avoid certain of the pitfalls identified in the trade association comments. Specifically, should the Commission choose to direct development of standards, APPA, *et al*. urge that they be governed by the following parameters:

- Standards should be 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;
- Standards must not require active management by utilities of third-party processes, nor hold utilities liable for vendor errors; and
- Utilities should be authorized to rely on credible attestations of their suppliers that they have honored identified security practices.

II. Comments

A. The Trade Association Initial Comments and Testimony at the Technical Conference Highlight Ongoing Efforts to Manage Upstream Risk and the Potential Pitfalls of Supply Chain Standards.

Members of APPA, *et al*. are well-aware of the risk that porous supplier security practices may pose to the BES. The trade associations' initial comments and testimony at the technical conference detail existing practices undertaken throughout the industry to help manage this risk. Further, as also pointed out by the trade associations, CIP-010-2 (cyber asset change management), which was approved by the Commission along with the suite of CIP Version 5 standards, provides a strong incentive for the industry to work with relevant suppliers to provide assurance regarding security practices associated with new cyber assets.[3]

Having said this, translating industry practice into a mandatory set of standards poses significant potential pitfalls, the most concerning of which would be enmeshing utilities in the

[3] *Id.*, pp. 19-21.

day-to-day security practices of their vendors. Calling for utilities effectively to act as design partners or operational foremen for equipment and software suppliers runs the risk of substantial confusion in design and manufacturing processes. An effort by FERC to exercise control over vendors or suppliers indirectly, through registered entities, could lead to costly inefficiencies, potentially reducing the field of available suppliers for essential products and services on which utilities rely.[4] Moreover, it is not clear that this undertaking lies within the core expertise of traditional utilities.

Further, since not all industrial control systems and associated hardware and software pose an equal risk to the BES, a standard that is overbroad in its reach with respect to the cyber assets it governs could add needlessly to the cost of supply inputs, with little associated security benefit.

B. Should the Commission Proceed to Direct Development of Supply Chain Standards, APPA, *et al*. ask that it Honor a Set of Key Limiting Principles.

If the Commission chooses to direct the development of standards addressing supply chain security, APPA, *et al*. ask that it honor the following set of limiting principles:

1. The Standards Must Be Risk-Based and Allow Utilities the Flexibility to Exercise Necessary Judgement in Identifying Upstream Risks to the BES.

Any standards ultimately developed must embody an approach that enables utilities to perform a risk assessment of the hardware and systems that create potential vulnerabilities to the BES. Similar to the approach taken in CIP-014-2, requirement R1 (Physical Security), utilities should be able to identify the assets that may pose a cyber risk to the BES, threatening "instability, uncontrolled separation or cascading outages." Not all control systems or

[4] *See* Pre-Filed Supply Chain Risk Management Technical Conference Testimony of the National Rural Electric Cooperative Association (p.3); Southern Co. (p.5); United Illuminating Co. (pp.4-5); Southern California Edison Co. (pp.3-4); and Pepco Holdings (p.5) (filed in Docket No. RM15-14-000).

information and communications technology pose this risk. This approach is consistent with NIST's Cybersecurity Framework, which prescribes a risk-based approach for critical infrastructure owners and operators to manage cybersecurity-related risk.[5]

2. The Standards Must Not Require Active Management by Utilities of Third-Party Processes, Nor Hold Utilities Liable for Vendor Errors.

It would be a mistake to call for utilities to manage actively the day-to-day security practices of their vendors. For reasons explained above and emphasized at the technical conference, utilities are not well-suited to directing their vendors' design and manufacturing processes. Putting utilities in this position runs the substantial risk of confusion in both the design and fabrication of critical facilities, leading to costly inefficiencies, potentially reducing the field of available suppliers for essential products and services on which utilities rely.[6] Further, that approach would risk calling upon utilities to act outside their core expertise, as utility managers may be required to interject themselves into manufacturing processes in which they have no special training.

Requiring utilities actively to manage third party processes would also run the risk of exceeding the boundaries of Federal Power Act section 215. As the Commission recognizes in the NOPR, its authority is bounded by the statute, which applies only to "users, owners and operators of the bulk-power system."[7] The more closely a standard comes to the actual control of supplier operations, even if indirect, the closer to the edge of its statutory authority the Commission would be.

---

[5] *See*: http://www.nist.gov/cyberframework/.

[6] *See* Pre-Filed Supply Chain Risk Management Technical Conference Testimony of the National Rural Electric Cooperative Association (p.3); Southern Co. (p.5); United Illuminating Co. (pp.4-5); Southern California Edison Co. (pp.3-4); and Pepco Holdings (p.5) (filed in Docket No. RM15-14-000).

[7] 16 U.S.C. 824o(b)(1). The Commission acknowledges this limitation in its NOPR when it states: "[a] reliability standard should not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities." NOPR at P 66.

For similar reasons, it would be unreasonable for any standard that FERC directs to hold utilities liable for the actions of third-party vendors or suppliers. While vendors should be responsible for the security of their work product, and while it is possible to devise a standard that calls for utilities to insist on such responsibility, the risk of error cannot reasonably be shifted to the regulated utility sector. Utilities can only reasonably be held liable for the administration of processes over which they have direct control.

3. Utilities Should Be Authorized to Rely on Credible Attestations of their Suppliers that They Have Honored Identified Security Practices.

An approach that calls for vendors to self-certify that they meet identified security parameters would simultaneously establish a standard of care on the suppliers' part, while avoiding a shift in liability to the utility sector, with its resultant inefficiencies and costs. Possibly, such certification may come with some form of third-party verification. This approach would avoid active management of vendors by utilities, work within the Commission's statutory authority, and place vendors in the position of standing by their products. APPA, *et al*. recommend leaving to the standards development process the substantive parameters for self-certification, as there are several models to choose from, including frameworks outlined by NIST and the Department of Energy.

III. Conclusion

For the foregoing reasons APPA, *et al*. urge the Commission, should it decide to direct the development of supply chain risk management standards, to ensure that these standards are carefully crafted to include the features described above.

Respectfully submitted,

Large Public Power Council
/s/Jonathan D. Schneider
Jonathan D. Schneider
Jonathan P. Trotta
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue NW, Suite 800
Washington, D.C. 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

Counsel for the
Large Public Power Council

American Public Power Association
/s/ Allen Mosher
Allen Mosher
Vice President, Policy Analysis
/s/ Randolph Elliott
Randolph Elliott
Regulatory Counsel
American Public Power Association
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
202-467-2900
amosher@publicpower.org
relliott@publicpower.org

Transmission Access Policy Study Group
/s/ Cynthia S. Bogorad
Cynthia S. Bogorad
Latif M. Nurani
Spiegel & McDiamid LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20005
202-879-4000

Counsel for the
Transmission Access Policy Study Group

Dated: April 19, 2016