UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Foundation for Resilient Societies	**)**	**Docket No. AD17-9-000**

COMMENTS OF THE TRADE ASSOCIATIONS

INTRODUCTION AND IDENTITY OF THE PARTIES

The American Public Power Association ("APPA"), Edison Electric Institute ("EEI"), Electricity Consumers Resource Council ("ELCON"), Electric Power Supply Association ("EPSA"), Large Public Power Council ("LPPC"), National Rural Electric Cooperative Association ("NRECA") and Transmission Access Policy Study Group ("TAPS") (together, the "Trade Associations"), on behalf of their members, hereby respond to the Notice of Petition for Rulemaking ("Notice") issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") soliciting comments on the Foundation for Resilient Societies' January 13, 2017 Petition for Rulemaking.[1] The Petition asks the Commission to initiate a rulemaking to require the development of an enhanced reliability standard to detect, report, mitigate, and remove malware from the Bulk Power System ("BPS").

The Trade Associations ask the Commission to reject the Petition. As discussed below, the Trade Associations firmly believe that the risks raised in the Petition are addressed by existing FERC-approved North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") reliability standards, and in ongoing dockets and standards developments processes currently being overseen by NERC and the Commission.

[1] *See Foundation for Resilient Societies*, Notice of Petition for Rulemaking, Docket No. AD17-9 (Jan. 17, 2017).

APPA is the national service organization representing the interests of not-for-profit, state, municipal and other locally owned electric utilities in the United States. One in seven electricity customers in the nation is served by public power. More than 2,000 public power utilities, operating in every state but Hawaii, collectively serve more than 49 million persons and account for over 15 percent of all electric energy (kilowatt-hours) sales to ultimate consumers. The primary goal of public power utilities is to provide customers in the communities they serve with reliable electric power and energy at the lowest reasonable cost, consistent with good environmental stewardship. This orientation aligns the interests of public power utilities with the long-term interests of the residents and businesses in their communities. Approximately 264 public power utilities are registered entities subject to compliance with NERC mandatory reliability standards.

EEI is the trade association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly and indirectly employ more than one million American workers. EEI's member companies invest more than $100 billion each year to build smarter energy infrastructure and to transition to even cleaner generation sources. EEI's members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to mandatory Reliability Standards developed and enforced by NERC. In addition to its domestic members, EEI has more than 60 international electric company members, and 250 industry suppliers and related organizations as Associate Members. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

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. Reliable electricity supply is essential to its members' operations.

Celebrating its 20th anniversary in 2017, EPSA is the national trade association representing leading independent power producers and marketers. EPSA members provide reliable and competitively priced electricity from environmentally responsible facilities using a diverse mix of fuels and technologies. Power supplied on a competitive basis collectively accounts for 40 percent of the U.S. installed generating capacity. EPSA seeks to bring the benefits of competition to all power customers. This pleading represents the position of EPSA as an organization, but not necessarily the views of any particular member with respect to any issue.

LPPC is an association of the 25 largest state-owned and municipal utilities in the nation. LPPC members are located throughout the nation, both within and outside RTO boundaries. LPPC represents the larger, asset-owning members of the public power sector.

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. NRECA's members participate in all of the organized wholesale electricity markets as well as single Balancing

Authority Areas 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 BPS.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[2] TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the Bulk Power System, 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.

Communications regarding these proceedings should be directed to the following:

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 EEI:
Melanie Seader,
Director, Reliability Policy
mseader@eei.org
Aryeh B. Fishman,
Associate General Counsel, Legal Regulatory Affairs
afishman@eei.org
EDISON ELECTRIC INSTITUTE
Washington, D.C. 20004
(202) 508-5000

For APPA:
Delia D. Patterson,
Vice President of Regulatory Affairs and General Counsel
dpatterson@publicpower.org
Randolph Elliott,
Senior Regulatory Counsel
relliott@publicpower.org
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000

For ELCON:
John P. Hughes
President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
jhughes@elcon.org

[2] 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.

Arlington, VA 22202
(202) 467-2900

For NRECA:
Paul M. Breakman,
FERC Counsel
paul.breakman@nreca.coop
Barry R. Lawson,
Sr. Director, Power Delivery and Reliability
barry.lawson@nreca.coop
NATIONAL RURAL ELECTRIC COOPERATIVE Association
4301 Wilson Boulevard
Arlington, VA 22203
703-907-5844

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

For EPSA:
Nancy Bagot,
Senior Vice President
Jack Cashin,
Director Regulatory Affairs
jcashin@epsa.org
ELECTRIC POWER SUPPLY ASSOCIATION
1401 New York Avenue, NW, Suite 1230
Washington, DC 20005
202-628-8200

COMMENTS

The Trade Associations are acutely aware of the danger posed to the BPS by malicious software ("malware"), yet ask the Commission to dismiss the Petition in deference to existing CIP standards, ongoing CIP dockets (including standards currently proceeding through the NERC standards drafting process), and other industry and government risk management efforts addressing malware risk. These efforts address the risks identified in the Petition in support of a new additional reliability standard.

Key among the standards already addressing this issue is Reliability Standard CIP-007-6, Requirement R3, which provides that "[e]ach Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-

007-6 Table R3 – Malicious Code Prevention." The requirement calls for Responsible Entities to: (1) deploy method(s) to deter, detect, or prevent malicious code; (2) mitigate the threat of detected malicious code; and (3) for those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns.

This standard is appropriately "performance based," that is, it prescribes what Responsible Entities must do, without specifying exactly how it should be done. In comments filed in Docket No. RM16-18, NERC explained that this approach is critical in connection with malware protection because of the wide range of equipment comprising the Bulk Electric System ("BES"), and the fast-moving target that evolving malware presents. NERC's Guidelines and Technical Basis for the approach taken in Reliability Standard CIP-007, R3, put the point this way:

> Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis, which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc.[3]

Other relevant requirements are spread throughout the CIP requirements, including required reporting of cybersecurity events.[4] As detailed by NERC in its response in Docket No. RM16-18, these requirements include Reliability Standards CIP-005-5, R1 (Electronic Security Perimeter); CIP-005-5, R2 (Protections for Interactive Remote Access); CIP-007-6, R1 (limiting and protecting accessible ports); and CIP-007-6, R2 (patch management required to detect

[3] Reliability Standard CIP-007-6, Guidelines and Technical Basis, at 4.

[4] *See* Reliability Standard CIP-008-5.

software vulnerabilities). In addition, in Order No. 822,[5] FERC recently approved new standards applicable to transient devices used in connection with High and Medium Impact BES Cyber Systems, while directing further development with respect to Low Impact BES Cyber Systems. And in Order No. 829,[6] FERC has directed new requirements to further address "supply chain" cybersecurity risks that may be posed by vendors. All of these efforts serve to proactively guard against the introduction of malware into BES Cyber Systems.

The Trade Associations and their members are well-aware of the malware risk and other potential vulnerabilities addressed in the February 25, 2016 Department of Homeland Security ("DHS") Alert, as well as the subsequent updates, that followed the cyberattack on the Ukrainian electric grid,[7] along with the ensuing joint E-ISAC/SANS report, on which a good deal of the Petition rests.[8] So too, of course, is the Commission, and this is now the subject to the July 21, 2016 Notice of Inquiry ("NOI") launched in Docket No. RM16-18.[9] NERC and the industry have responded to the NOI, and recommended that the Commission await the further study that NERC has undertaken, recognizing that there are operational consequences to the approaches under consideration. Whatever the outcome, it is clear that the range of vulnerabilities NERC is currently studying substantially overlaps those raised in the Petition. This engagement by NERC, the industry, and the Commission supports the conclusion that informed action is being

[5] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61, 037 (2016) ("Order No. 822").

[6] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016) ("Order No. 829").

[7] *See* DHS ICS-CERT Alert: Cyber-Attack Against Ukrainian Critical Infrastructure (Feb. 25, 2016), available at: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[8] SANS INDUS. CONTROL SYS., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID (Mar. 18. 2016), available at https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[9] The focus of that NOI is on any additional measures that may be taken to further isolate control centers, and on the utility of application "whitelisting," a technique designed to prevent unauthorized programs from running on cyber systems. *Cyber Systems in Control Centers*, Notice of Inquiry, 156 FERC ¶ 61,051 (2016).

taken in response to identified cybersecurity risks in a manner that balances potential impacts to the ongoing operation of the grid, the interference with which would pose a reliability concern itself.

The Trade Associations also note that the Petition suggests, incorrectly, that existing Reliability Standards do not address distribution level assets that may impact the BES.[10] In fact, Reliability Standard CIP-007-6 (including Requirement R3) applies to Distribution Providers' operating facilities, systems and equipment needed for the protection or restoration of the BES.[11]

Further, as to the Petition's assertion (pp. 12-13) that there are gaps with respect to communications systems, the Trade Associations note, first, that high and medium impact cyber systems owned and/or operated by Responsible Entities are subject to compliance with CIP-007-5, R3. To the extent that the Petition is referring to communications networks that are outside Responsible Entities' control, FERC's statutory reach under the Federal Power Act is limited. Nonetheless, the Trade Associations note that associated cyber vulnerabilities are currently being considered in conjunction with Docket No. RM16-18. The Commission should defer here to the study being undertaken in that docket.

Finally, the Trade Associations note that, in addition to the mandatory CIP Reliability Standards, electric utilities routinely work with voluntary cybersecurity frameworks, such as the National Institute of Standards and Technology ("NIST") Cybersecurity Framework and the Department of Energy ("DOE") Cybersecurity Capability Maturity Model. These enterprise-wide frameworks and the tools used to implement them allow electric companies to assess their cybersecurity capabilities and to prioritize their human and technological resources to

[10] Petition at 13, 15.

[11] *See* Reliability Standard CIP-007 (Applicability), Sections 4.1.2, 4.2.1.

continually strengthen their security posture. In addition to these voluntary undertakings, electric utilities partner with the White House and federal agencies – including DOE, DHS, Department of Defense, FERC, and the Federal Bureau of Investigation – to improve sector-wide response to cyber threats. This includes information sharing and collaboration with NIST and federal intelligence and law enforcement agencies that further strengthen cybersecurity capabilities and posture.

Additional senior management attention to cyber risks is directed through the work of the Electricity Subsector Coordinating Council ("ESCC"), a CEO-level group that serves as the primary liaison between the federal government and the electric sector to address national security threats to the grid. The ESCC is focused on several key areas, including planning and exercising coordinated responses to grid attacks; ensuring that threat information is communicated quickly among government and industry stakeholders; deploying government technologies on utility systems that improve situational awareness of threats to the grid; and cross-sector coordination with the other critical infrastructure sectors.

These collaborative industry and government risk management efforts provide timely and effective ways to address evolving threats and vulnerabilities supplementing the Reliability Standards. The ESCC, for example, served as the vehicle by which the industry's government partners shared intelligence regarding distributed denial of services attacks on non-utility systems. That information was, in turn, shared more broadly throughout the industry by the Electricity Information Sharing and Analysis Center ("E-ISAC"). The ESCC has also served as an effective channel for continuous intelligence sharing on malicious activity, the communication of which has been amplified by the E-ISAC, along with additional technical indicators and mitigation strategies.

The Cybersecurity Risk Information Sharing Program ("CRISP") provides further timely sharing of threat information to utilities serving more than 75% of all electricity customers.[12] This information is further shared by the E-ISAC more broadly with all utility members.[13]

CONCLUSION

The Trade Associations appreciate the Petitioner's effort to focus attention on malware risk, and share Petitioner's interest in enhancing the security of the grid. But the Petition understates the reach of existing standards, the potential impact of new standards under development and study, and the breadth of cybersecurity efforts across the industry and government, including those that have been voluntarily undertaken. For these reasons, the Trade Associations ask the Commission to reject the Petition.

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, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

Edison Electric Institute

/s/ David K. Owens
David K. Owens,
Executive Vice President, Business Operations
Melanie Seader,
Director, Reliability Policy
mseader@eei.org
Aryeh B. Fishman,
Associate General Counsel, Legal Regulatory Affairs
afishman@eei.org
EDISON ELECTRIC INSTITUTE
Washington, D.C. 20004
(202) 508-5000

[12] The Petition's representation (p. 9) that CRISP reaches utilities serving "less than half of America's electricity customers" is inaccurate. *See* Statement of Scott Aaronson before the House Energy and Commerce Comm. Subcomm. on Energy, 115th Cong. 9 (2017) ("The Electricity Sector's Efforts to Respond to Cybersecurity Threats"), available at http://docs.house.gov/meetings/IF/IF03/20170201/105497/HHRG-115-IF03-Wstate-AaronsonS-20170201.pdf.

[13] *Id.*

American Public Power Association

/s/ Delia D. Patterson
Delia D. Patterson,
Vice President of Regulatory Affairs and General Counsel
dpatterson@publicpower.org
Randolph Elliott,
Senior Regulatory Counsel
relliott@publicpower.org
AMERICAN PUBLIC POWER ASSOCIATION
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
(202) 467-2900

Electricity Consumers Resource Council

/s/ John P. Hughes
John P. Hughes
President & CEO
ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
jhughes@elcon.org

National Rural Electric Cooperative Association

/s/ Paul D. Breakman
Paul M. Breakman,
FERC Counsel
paul.breakman@nreca.coop
Barry R. Lawson,
Sr. Director, Power Delivery and Reliability
barry.lawson@nreca.coop
NATIONAL RURAL ELECTRIC COOPERATIVE Association
4301 Wilson Boulevard
Arlington, VA 22203
703-907-5844

Transmission Access Policy Study Group

/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
cynthia.bogorad@spiegelmcd.com
latif.nurani@spiegelmcd.com

Electric Power Supply Association

/s/ Nancy Bagot
Nancy Bagot,
Senior Vice President
Jack Cashin,
Director Regulatory Affairs
jcashin@epsa.org
ELECTRIC POWER SUPPLY ASSOCIATION
1401 New York Avenue, NW, Suite 1230
Washington, DC 20005
202-628-8200

Dated: February 17, 2017