UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cyber Systems in Control Centers	**)** **)** **)** **)** **)**	**Docket No. RM16-18-000**

COMMENTS OF THE EDISON ELECTRIC INSTITUTE, THE ELECTRIC POWER SUPPLY ASSOCIATION, AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

Edison Electric Institute ("EEI"), the Electric Power Supply Association ("EPSA"), and the National Rural Electric Cooperative Association ("NRECA"), (collectively, the "Trade Associations") on behalf of our member companies, respectfully submit these comments, in response to the Notice of Inquiry ("NOI") issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") on July 21, 2016, in the above-referenced docket.[1] In the NOI, the Commission seeks comments on possible modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards regarding the cybersecurity of Control Centers[2] used to monitor and control the bulk-power system and any potential impacts on the operation of the bulk-power system resulting from such modifications.

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 employ more than 500,000 workers. With more than $85

[1] *Cyber Systems in Control Centers*, Notice of Inquiry, 156 FERC ¶ 61,051 (2016).

[2] NERC defines "Control Center" as "[o]ne or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers…." NERC Glossary of Terms Used in Reliability Standards (May 17, 2016) at 33 ("NERC Glossary").

billion in annual capital expenditures, the electric industry is responsible for millions of jobs related to the delivery of power, including the construction of modified or new infrastructure. Reliable, affordable, and sustainable electricity powers the economy and enhances the lives of all Americans. EEI also has 70 international electric companies as Affiliate 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. EEI members are subject to mandatory Reliability Standards developed and enforced by the North American Electric Reliability Corporation ("NERC").

EPSA is the national trade association representing leading competitive power suppliers, including generators and marketers. Competitive suppliers, which collectively account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities. 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.

NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent from non-NRECA members. The vast majority of NRECA members are not-for profit, consumer-owned cooperatives. NRECA's members also include 65 generation and transmission ("G&T") cooperatives, which generate and transmit power to 668 of the 838 distribution

cooperatives. The G&Ts are owned by the distribution cooperatives they serve. Remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost. NRECA members are directly affected by the proposed Reliability Standards developed and enforced by NERC.

BACKGROUND

As predicate for this inquiry, the NOI states that on December 23, 2015, three regional electric power distribution companies in the Ukraine experienced a cyberattack resulting in power outages.[3] In response to this event, the U.S. Department of Homeland Security ("DHS") Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT) issued an "Alert,"[4] with a number of mitigation measures for organizations to consider.[5] Subsequently, on July 21, 2016, the Commission issued its NOI seeking comments in the above-captioned docket. The NOI states that, while certain controls in the CIP Reliability Standards may reduce the risk of cyberattacks on cyber systems used extensively for the operation and maintenance of interconnected transmission networks,[6] the Commission seeks comment on whether additional controls should be required through modifications to the CIP Reliability Standards regarding

[3] NOI at PP 4-5.

[4] Department of Homeland Security, Alert (IR-ALERT-H-16-056-01) Cyber Attack Against Ukrainian Critical Infrastructure (February 25, 2016) (Alert), available at https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[5] NOI at PP 4-6.

[6] Cyber systems are referred to as "BES Cyber Systems" in the CIP Reliability Standards. The NERC Glossary defines "BES Cyber Systems" as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC Glossary at 15. The NERC Glossary defines "BES Cyber Asset" as "[a] Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems." *Id*.

cybersecurity of Control Centers[7] used to monitor and control the bulk-power system and any potential impacts on the operation of the bulk-power system resulting from such modifications. In particular, the NOI asks for comment on the following modifications to the CIP Reliability Standards to require: (1) separation between the Internet and Bulk Electric System ("BES") Cyber Systems in Control Centers performing transmission operator functions; and (2) computer administration practices that prevent unauthorized programs from running, referred to as "application whitelisting," for cyber systems in Control Centers. In response, the Trade Associations offer the following comments.

COMMENTS

The Trade Associations appreciate the Commission's decision to issue a NOI to examine the need for, and possible effects of, modifications to the CIP Reliability Standards regarding Control Centers used to monitor and control the bulk-power system in real time. The Trade Associations support the Commission's continued attention to the threat of attacks to cyber systems used to operate and maintain interconnected networks that pose a real threat to grid reliability. The Commission is wise to have avoided rushing directly to a Notice of Proposed Rulemaking to require the development of modifications to the CIP Reliability Standards. The NOI is an appropriate action for the Commission to take given its responsibilities and in view of the importance and complexity of this issue. The Commission should proceed cautiously and thoughtfully before directing the development of a reliability standard to address these threats.

The Trade Associations agree with the Commission that the Ukrainian cyberattack staged in 2015 on the electric grid in the Ukraine demonstrated how "[i]nterconnected networks, unless

[7] NERC defines "Control Center" as "[o]ne or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers…." NERC Glossary of Terms Used in Reliability Standards (May 17, 2016) at 33 ("NERC Glossary").

adequately protected, may be vulnerable."[8] The Trade Associations also support the Commission's effort to examine whether the cyber systems used to operate and maintain interconnected networks in the United States are adequately protected against a similar cyberattack before considering whether additional controls should be required. The Trade Associations appreciate the work done by researchers from DHS as well as other entities (e.g., the NERC, E-ISAC and SANS)[9] to share what happened during the cyber-attack in Ukraine and the mitigation measures employed during that event. Lessons learned from cyber incidents, even those from other countries, are valuable to the electric sector in reviewing and improving their existing protection, detection, response, and recovery strategies. The lessons learned developed by the researchers who investigated the attack in Ukraine have helped validate the effectiveness of the existing CIP Reliability Standards.[10] Accordingly, it is very important that the Commission develop a full record regarding the potential benefits and adverse impacts of the additional protections described in the NOI, and the Trade Associations hope that our comments assist the Commission in this regard.

While we support the Commission's analysis, we do not consider either of these measures compelling solutions (i.e., Internet isolation or application whitelisting) that might represent any tangible improvements over what is already required in the current body of CIP Reliability Standards. Moreover, such requirements, if imposed, could create serious operational limitations affecting even routine communications and data sharing. The Trade Associations are

[8] NOI at P1.

[9] *See e.g.*, E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid (March 18, 2016) at 3, http://www.nerc.com/pa/CI/ESISAC/Documents/EISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

[10] *See e.g.*, SANS Industrial Control Systems Security Blog, *Ukrainian Grid Attack: How NERC CIP-like Measures Might Have Helped* (March 24, 2016), available at https://ics.sans.org/blog/2016/03/24/ukrainian-grid-attack-how-nerc-cip-like-measures-might-have-helped

also concerned that applying unproven and highly prescriptive malware solutions to BES Cyber Systems within control centers could pose substantial reliability risk to the very systems the Commission hopes to protect. While the Trade Associations have little doubt that the use of these mitigations may be suitable for certain applications and situations, their broader application should be determined by the subject matter experts ("SMEs") responsible for designing and protecting owner and operator BES Cyber Systems, and not required by regulatory compliance.

The Trade Associations are also concerned that additional directives at this time would increase an already significant workload for the industry with respect to implementation of and, development of modifications to, CIP Reliability Standards. It is important to note that significant industry resources are currently allocated to implementation of the CIP Reliability Standards. The implementation of version 6 of the CIP Cyber Security Standards ("CIP version 6") is new and for some systems (i.e., low impact BES Cyber Systems) CIP implementation is just beginning. Additionally, enforcement by NERC, Regional Entities, and FERC of CIP version 6 has just begun. Furthermore, CIP version 6 is already under modification from two orders by the Commission, Order Nos. 822 and 829.[11] The Trade Associations urge the Commission to carefully consider the potential impacts that additional modifications (i.e., a third standards drafting process in parallel with the other two) will have on the reliability of the bulk-power system and to seek alternatives to further modifications.

Accordingly, it is very important that the Commission develop a full record regarding the potential benefits and adverse impacts of the additional protections described in the NOI. It is in

[11] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 (2016), *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016).

this context that the Trade Associations are providing these comments, which we hope will help inform the Commission in deciding the most appropriate next steps, if any.

I. The existing CIP Reliability Standards already address the DHS ICS-CERT Alert recommendations and new isolation requirements may not be possible and may negatively impact grid modernization, security, and reliability

The NOI seeks comments on whether to modify the CIP Reliability Standards to mandate as an additional protection the separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions through use of physical (hardware) or logical (software) means.[12] The NOI acknowledges that requiring physical separation between the Internet and cyber systems in Control Centers performing transmission operator functions would require data connections to Control Centers or other facilities owned by transmission operators over dedicated data lines owned or leased by transmission operators, rather than allowing communications over the Internet.[13] The NOI also asks for comment on the operational impact to the bulk-power system if BES Cyber Systems were isolated from the Internet in Control Centers performing transmission operator functions as well as what, if any, reliability issues might arise from such a requirement.[14]

A. The CIP Reliability Standards already limit connectivity to BES Cyber Systems from untrusted networks such as the Internet

The Trade Associations do not believe the CIP Reliability Standards should be modified to require isolation because they already provide appropriate levels of separation between BES Cyber Systems and untrusted networks (e.g., the Internet) through logical controls that limit connectivity to BES Cyber Systems.

[12] NOI at P 7-10.

[13] *Id*. at P 10.

[14] *Id*. at P 11.

The DHS ICS-CERT Alert recommended that organizations "isolate ICS networks from any untrusted networks, especially the Internet"—this is the security objective—and then specifically recommended four types of isolation measures (i.e., potential controls): (1) "[a]ll unused ports should be locked down and all unused services turned off," (2) "[i]f a defined business requirement or control function exists, only allow real-time connectivity to external networks," (3) "[i]f one-way communication can accomplish a task, use optical separation ('data diode')," and (4) "[i]f bidirectional communication is necessary, then use a single open port over a restricted network path."[15] These are all logical controls, which are already required by the existing CIP Reliability Standards.

The Commission acknowledged that the current CIP Reliability Standards already provide necessary controls regarding unused ports, but did not discuss explicitly their specific views of the other controls identified in the NOI. However, we believe that those controls are broadly covered by the existing standards. Specifically, connectivity to external networks is controlled by electronic access controls found in CIP-003-6, CIP-004-6, CIP-005-5, and CIP-007-6. Furthermore, CIP-005-5 Requirement 1 limits connectivity to external networks, with specific controls for external routable connectivity and dial-up connectivity. While External Routable Connectivity[16] is limited by definition to bi-directional communications, some utilities have leveraged data diodes (one-way optical separated communications) for certain limited applications, which is allowed under the existing CIP Reliability Standards as an alternative to the external routable connectivity security requirements. The DHS ICS-CERT Alert specifically

[15] Alert at Mitigation Section.

[16] External Routable Connectivity is defined as "the ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." NERC Glossary of Terms Used in NERC Reliability Standards.

recommended that "[i]f one-way communication can accomplish a task, use optical separation" and "if bidirectional communication is necessary, then use a single open port over a restricted network path."[17] The existing CIP Reliability Standards enables utilities to evaluate whether a data diode is an appropriate technology solution for the specific task and if it is not, then the CIP requirements address the security risk inherent to bidirectional communications. The Trade Associations also strongly caution the Commission against directing modifications that require specific technologies (e.g., data diodes) or methods (i.e., a "how") to meet a security objective (i.e., "the what").

Given that the existing security controls described above and contained within the CIP Reliability Standards already provide the isolation controls suggested by the DHS ICS-CERT Alert, it is not clear what remaining gaps the Commission is seeking to remedy. And therefore we are assuming the Commission is asking whether additional isolation requirements are necessary or prudent. So in this context, we do not believe additional isolation requirements are necessary or would even provide sufficient security benefits to merit adding such rigid new requirements to the CIP Reliability Standards.

B. Compliance with new isolation requirements may not be possible or practical

The Trade Associations appreciate that the NOI seeks to understand that any security benefit provided through the use of new isolation requirements must be considered in view of the operational and reliability impacts. The Trade Associations believe that new isolation requirements will place considerable burdens on many companies, while in some cases it may not even be possible or practical given how most modern telecommunications system are

[17] Alert at Mitigation Section.

designed and built.

Internal telecommunication systems are broadly shared networks (e.g., SONET, MPLS, Channel Banks, Microwave Systems,) delivering a wide range of internal services for both grid operations and applications that depend on Internet access. Complete physical isolation may require companies to build separate telecommunication networks (i.e., one serving BES Cyber Systems and one serving everything else). Although technically possible, the cost would be considerable while yielding relatively questionable security benefits. Furthermore, for those companies who own and operate expansive and complex private networks, most still rely on commercial carrier services to fill the gaps in coverage within their own networks. Also, leased telecommunication services in many areas are limited, which places constraints on the type and manner of service that can be leased. For these reasons, physical isolation would be inefficient and largely impractical, both for large and small entities alike.

It is also important to recognize that while many of these dedicated leased telecommunication services are considered dedicated services and largely isolated from the Internet, they are in fact transported over shared networks that largely contain a mix of services, including Internet applications. While the Trade Associations believe that these systems and services can be securely used for BES Cyber Systems, new isolation requirements could limit the use of these systems.

The Commission also seeks comment on whether and how physical isolation requirements might affect a transmission operator's communications with its reliability coordinator ("RC") or other applicable entities required under the Reliability Standard.[18] While utilities may interconnect facilities and other Control Centers with dedicated leased lines, nearly

[18] NOI at P 11.

all other forms of communications used within Control Centers often leverage Internet based communications in some manner (e.g., transfer of data, non-SCADA equipment monitoring, remote access and troubleshooting to devices such as protective relays, voice communications (wired and wireless), etc.).[19] Furthermore, requiring physical isolation from the Internet would hinder transmission operating personnel from having access and visibility into voltage schedules, reliability directives, and other information made available through RTO's or RC's websites accessible through the Internet. The Trade Associations also understand that isolation of Control Centers from the Internet would also negatively impact routine and emergency communications such as those described in IRO-001-1.1 (Reliability Coordinator – Responsibilities and Authorities) Requirement R8; TOP-001-1a (Reliability Responsibilities and Authorities) Requirement R3; and VAR-002-4 (Generator Operation for Maintaining Network Voltage Schedules) Requirement R2.

C. New requirements to further isolate BES Cyber Systems in Control Centers from untrusted networks such as the Internet could negatively impact grid modernization, security, and reliability

Complete physical isolation from untrusted networks, such as the Internet, would also introduce new reliability challenges as well as barriers to the grid modernization efforts essential to meeting many of the goals identified in the DOE's Quadrennial Energy Review.[20] These grid modernization efforts require a more open system that allows access, interconnection, and communication to a whole host of new grid participants, such as renewable resources and energy storage. Such a vision is not possible with closed or completely isolated systems.

Electric sector utilities use a complex mix of internal and leased communications

[19] Additionally, systems such as the Open Access Same-Time Information System ("OASIS") are also Internet based.

[20] DOE, *Quadrennial Energy Review: Energy Transmission, Storage and Distribution Infrastructure* (April 2015).

supporting their transmission operations. These systems include their utility data networks, backbone communications systems, mobile radio systems, voice communications such as VoIP, data transport from a wide range of assets and systems used by the bulk-power system, and communications to a growing number of non-utility participants. Utility networks are also supported by a range of leased telecommunication services to supplement their communication needs when companies cannot economically build their own private systems. Whether supporting private or leased services, systems vary in forms and degrees of isolation from the Internet, but embedded in these systems is the dual need for owners and operators to both maintain and document compliance with the requirements of the CIP Reliability Standards and to ensure that the core systems used for transmission operations remain secure and reliable on a day-to-day basis. For these reasons, the Trade Associations are concerned that any new requirements that might impose broad and prescriptive isolation from the Internet, in any form, might needlessly hinder the use of these critical systems, creating operational challenges for many companies. While these operational challenges would create significant difficulties for even the largest of entities, their impacts would be even greater for smaller entities with fewer resources and a limited ability to build their own private networks and systems.

The Commission should also give careful consideration to the growing dependence companies have on many services and products that routinely leverage the ubiquitous communications offered by the Internet. Advancements to bulk-power system reliability and security may only be possible through the broad use of communications supported by the Internet or other shared networks. For example, some vendor services may require secure connectivity to some BES Cyber Systems to help manage certain security services. This access is already controlled by the existing CIP Reliability Standards, and new requirements will be

added under the Order No. 829 modifications.

Additionally, dedicated, point-to-point communications do not necessarily provide the redundancy advantages often provided by routable-based communications that leverage interconnected networks (e.g., Internet). Specifically, point-to-point communications is often provided without routing diversity and frequently has embedded single points of failure. While Internet based communications can also have similar weaknesses those weaknesses are less prevalent due to the expansiveness of those networks. For these reasons, the Trade Associations encourage the Commission to not limit these options but rather to allow the protections already in place in the CIP Reliability Standards to prove effective while permitting responsible entities the discretion needed to make security and communication choices that both meet their needs and are appropriately secure.

New isolation requirements could have a negative impact on the continued modernization of the bulk-power system while providing new untenable restrictions to both traditional and renewable resource owners, who are becoming an increasingly important part of the resource mix in many areas. The Trade Associations believe that, over time, Internet-based communications will become an increasing and important method of communication, driving all forms of grid modernization. Although these communications systems require security controls, as provided by the CIP Reliability Standards, the Trade Associations do not believe that applying new requirements mandating isolation from the Internet can be effectively applied without creating substantial new burdens onto resource owners. While requiring isolation from the Internet may appear to offer some security improvements, the Trade Associations believe that those improvements would be small in comparison to the newly created operational challenges and compromises made to both resiliency and redundancy.

II. Requiring the use of application whitelisting in Control Centers is unnecessary, could cause significant compliance and reliability issues for owners and operators of BES Cyber Systems in Control Centers, and is not appropriate for all BES Cyber Systems in Control Centers

The Commission seeks comment on whether the CIP Reliability Standards should be modified to require application whitelisting for all BES Cyber Systems in Control Centers.[21] The Trade Associations believe that requiring application whitelisting would limit a responsible entity's ability to select the most effective protections to secure their BES Cyber Systems and may prove substantially less effective than allowing entities to evaluate and select a suite of security solutions more tailored for their own unique operating environment. Moreover, the Trade Associations understand that application whitelisting on industrial control systems used within the electric sector is an emerging technology.

While the Trade Associations support the Commission's desire to enhance BES Cyber System security, application whitelisting is simply one of many solutions available to companies and the DHS ICS-CERT Alert did not recommend the broad deployment of application whitelisting. Instead, the Alert encouraged companies to "work with their vendors to baseline and calibrate [application whitelisting] AWL" for possible future use on some systems which might be particularly suited to this type of application.[22] Therefore, the Commission should not take any action that inhibits the ability of companies to assess and select solutions that best protect their BES Cyber Systems and should not direct modifications to the CIP Reliability Standards to require application whitelisting in Control Centers.

Again, the Trade Associations strongly caution the Commission against directing

[21] NOI at P 15.

[22] Alert at Mitigation Section.

modifications that require specific technologies or methods (i.e., a "how") to meet a security objective (i.e., "the what"). Application whitelisting is a method to detect and/or prevent malicious code from running on a Cyber Asset. There are a number of technologies and methods for deterring, detecting, and preventing malware, which should be considered based on the capabilities of the Cyber Asset, the system and environment it operates in, and the risk where it is deployed. BES Cyber Systems in Control Centers include both static and dynamic systems, which may make certain applications inappropriate for application whitelisting solutions. The existing CIP Reliability Standards allow for this tailored approach to deter, detect, or prevent malicious code.[23] The standard drafting team specifically addressed whitelisting in the guidelines and technical basis for CIP-007-6:

> 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.

Therefore, requiring application whitelisting would be mandating a specific method (among those listed above) for achieving a particular outcome (i.e., the "how" instead of the "what"), instead of giving due deference to the technical expertise of NERC and the industry to achieve the desired outcome.

The Trade Associations also understand that most of the EMS/SCADA systems that are used within electric utility Control Centers currently have limited capability to deploy application whitelisting. The Trade Associations have found, as a result of conversations with EMS/SCADA vendors, that most such vendors are unaware of any successful deployments of application whitelisting in the electric utility sector. Therefore, new deployments of application whitelisting need to be supported by substantial testing and piloting prior to use of this technology. The Trade Associations are also concerned that applying untested anti-malware applications within Control Centers prematurely could have significant security and reliability impacts. For example, the use of application whitelisting for preventing malware could hinder restoration efforts during emergency operations. While some EMS/SCADA manufacturers and customers are evaluating and investigating the compatibility of application whitelisting, it is unclear how or if these systems are suitable to run effectively on all BES Cyber Systems in Control Centers.

SCADA/EMS systems are developed by a wide range of vendors necessitating their direct involvement as to whether their systems could support this type of malware protection. Using application whitelisting as a malware prevention tool also increases responsible entity reliance on these vendors to provide updates and troubleshooting. Increasing reliance on third parties such as vendors requires granting greater connectivity, access, and control of those systems to those third parties (e.g., vendor remote access controls) that would be hindered (if not rendered ineffective) by the NOI's suggestion of further isolation from the Internet. Responsible entities must carefully balance the risks introduced by the mitigation options with the potential security benefits. The existing CIP Reliability Standards enable this balanced approach while ensuring that BES Cyber Systems are well protected from cyber threats.

Given that application whitelisting is already an option for mitigating risk under the existing CIP Reliability Standards and the fact that it is a new technology that may not be appropriate for use on all BES Cyber Systems in Control Centers, the Trade Associations do not support modification of the CIP Reliability Standards to require application whitelisting.

III. The Commission should consider alternatives to CIP Reliability Standards modifications for improving bulk-power system reliability

The Trade Associations would like to emphasize that utilities are continually working at improving their security solutions in order to enhance and refine their security solutions to protect BES Cyber Systems. While some of the methods discussed in the NOI may have some appropriate applications for particular systems in particular circumstances, the Commission must consider the potential implications of issues prescriptive controls before mandating new directives that will increase an already significant workload for NERC and industry. The industry is expending substantial technical and compliance resources to not only ensure compliance with the large number of new requirements in CIP version 6, but also to ensure the successful development of the modifications already directed by the Commission.

Further modifications to CIP version 6 may only serve to diminish reliability by not allowing the industry to effectively adapt and become proficient in implementation and compliance with the requirements that are both existing and under development. The Trade Associations believe that there has not been sufficient time for the industry, NERC, Regional Entities, and the Commission to assess the strengths and weaknesses of the CIP version 6 requirements as implemented and under modification.

The Trade Associations are concerned that continuous modification of the CIP Reliability Standards will drive the industry's skilled security professionals to focus on regulatory compliance rather than the security and reliability of the bulk-power system. This will reinforce

a culture of compliance over the culture of security that many entities have been building using the CIP Reliability Standards as a foundation, which will hamper industry's ability to adapt and innovate as the threat landscape changes. For this reason, the Commission should consider the current pace of change and allow entities the needed time to fully apply the growing number of new requirements, both those approved and being developed. Such an approach will allow Responsible Entities, NERC, Regional Entities, and the Commission to accurately assess how these changes are improving the security and reliability of the bulk-power system and make informed decisions as to whether modifications are needed to improve reliability.

Moreover, the industry needs a steady state and sufficient time to implement, and to assess the effectiveness of the CIP version 6 and the already directed modifications before new modifications should be considered. In the meantime, the Commission may want to consider increasing engagement with NERC, Regional Entities, industry trade associations, and responsible entities through venues such as the Commission led audits, meetings, and technical workshops to better understand industry security controls and practices and identify alternative approaches (i.e., other than CIP modifications) to continue to improve bulk-power system reliability and security. The Commission should also consider non-regulatory venues such as the Electricity Subsector Coordinating Council to engage industry on emerging security issues and new approaches to mitigating bulk-power system risk.

The Trade Associations believe that industry engagement provides a better, security-focused approach to bulk-power system reliability that will allow the industry the time it needs to finish implementing and modifying CIP version 6 as well as allow NERC, Regional Entities, and the Commission to accurately assess whether modifications are necessary.

CONCLUSION

WHEREFORE, for the foregoing reasons, the Trade Associations request that the Commission ensure that any future action ordered as a result of this proceeding is consistent as discussed above.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ 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

ELECTRIC POWER SUPPLY ASSOCIATION

/s/ Nancy Bagot
Senior Vice President
Jack Cashin
Director, Regulatory Affairs
Jcashin@epsa.org
Electric Power Supply Association
1401 New York Ave., NW, Suite 1230
Washington, DC 20005
(202) 628-8200

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

/s/ Paul M. Breakman
Paul M. Breakman, Senior Director – FERC Counsel
paul.breakman@nreca.coop
Barry R. Lawson, Senior Director, Power Delivery and Reliability

barry.lawson@nreca.coop
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
703-907-5844

Dated: September 26, 2016

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 26th day of September.

/s/ Aryeh B. Fishman
Aryeh B. Fishman
Associate General Counsel, Regulatory Legal Affairs
Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000
afishman@eei.org