UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security	)	Docket No. RM20-19-000

COMMENTS OF
THE AMERICAN PUBLIC POWER ASSOCIATION,
THE LARGE PUBLIC POWER COUNCIL,
THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND
THE UTILITIES TECHNOLOGY COUNCIL

The American Public Power Association ("APPA"), the Large Public Power Council ("LPPC"), the National Rural Electric Cooperative Association ("NRECA"), and the Utilities Technology Council ("UTC") (collectively, the "Joint Trade Associations") submit these comments in response to the Notice of Inquiry ("NOI") issued by the Federal Energy Regulatory Commission ("Commission") on September 17, 2020 in the above-captioned docket concerning potential risks to the Bulk Electric System ("BES") from equipment and services produced or provided by certain entities identified as risks to national security.[1] Joint Trade Associations appreciate the opportunity to comment on the important questions raised in the NOI, and we provide our collective response below.

I. INTRODUCTION

Building on recent executive orders, legislation, and other federal agency actions, the Commission seeks industry input on potential risks posed by equipment and services produced or provided by certain specific entities that have been identified as risks to national security

[1] *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, 172 FERC ¶ 61,224 (2020).

("Covered Companies").[2] The NOI requests industry comment on six issues: (1) the extent of the use of equipment and services provided by the Covered Companies related to BES operations; (2) the risks to BES reliability and security posed by such equipment and services; (3) whether the North American Electric Reliability Corporation ("NERC") Critical Infrastructure Protection ("CIP") Reliability Standards adequately mitigate any identified risks; (4) mandatory actions the Commission could consider taking to mitigate the risk to BES operations from equipment and services provided by the Covered Companies; (5) information on strategies that entities have implemented or plan to implement beyond compliance with the CIP standards to mitigate risks associated with use of equipment and services provided by the Covered Companies; and (6) other methods the Commission may employ to address these issues, including collaboration with industry to raise awareness about the identified risks and assistance with mitigating actions, such as by facilitating information sharing.[3]

Joint Trade Associations appreciate the Commission's efforts to assess the risk posed by Covered Companies equipment and services. We note at the outset, however, that electric utilities face certain challenges in responding to the Commission's inquiries, including the fact that much of the equipment provided by the Covered Companies may be used in communications networks that are not owned or operated by electric utilities. The most comprehensive source of information concerning the extent to which equipment and services

[2] The Covered Companies specifically identified in the NOI are Huawei Technologies Company ("Huawei"); ZTE Corporation ("ZTE"); Hytera Communications Corporation; Hanzhou Hikvision Digital Technology Company; and Dahua Technology Company. NOI at PP 3, 11. Covered Companies would also include an entity that produces or provides telecommunications or video surveillance equipment or services that is "an entity that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the . . . People's Republic of China." *Id* at P 11 (quoting John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018)). The equipment and services provided by Covered Companies may include both operating technology systems and business information technology systems.

[3] NOI at P 4; *see also id.* at P 20.

provided by the Covered Companies are presently used in BES operations is likely to be the industry response to NERC's July 8, 2020 Level 2 Alert associated with Executive Order 13920.

Further, while the NOI asks a series of questions about the risks that may be posed by the use of Covered Companies equipment or services, the best source of such information is likely to be federal intelligence and law enforcement authorities, on whom electric utilities must ultimately rely for timely and actionable information about the potential risks of equipment with foreign ownership, control, or influence. As a general matter, however, we observe that the ongoing risks to the BES likely have already been moderated by the prior federal actions described in the NOI, which have alerted the industry to the potential risks associated with using equipment or services from Covered Companies.[4]

NERC's existing and pending CIP standards, and likely future Department of Energy regulations resulting from Executive Order 13920, provide an appropriate baseline set of requirements, processes, and procedures to help guard against risks associated with equipment and services from the Covered Companies.[5] We caution the Commission against directing NERC to develop new standards or requirements in an effort to mitigate these risks. Given that electric utilities use various approaches to provide telecommunications services on their systems, there is unlikely to be a "one size fits all" approach to addressing these risks. Further, indirectly imposing obligations on telecommunications providers through mandatory CIP standards could conflict with telecommunication mandates or protocols and potentially reduce the willingness of

[4] *See* NOI at PP 5-14.

[5] Joint Trade Associations note that the recent comments filed by APPA and LPPC in Docket No. RM20-12-000 addressing the risks of coordinated cyber-attack also provide information that may be germane to consideration of the adequacy of current NERC CIP standards in mitigating the potential risks posed by Covered Companies equipment and services. *See Potential Enhancements to the Critical Infrastructure Protection Reliability Standards*, Docket No. RM20-12-000, Comments of the American Public Power Association and Large Public Power Council at 18-30 (Aug. 24, 2020).

telecommunications providers to serve electric utilities.

Finally, As the Commission rightly suggests in the NOI, information sharing by federal authorities is essential in allowing electric utilities to identify and mitigate potential risks from equipment or services supplied by entities that may pose a threat to national security.

II. INTEREST OF THE JOINT TRADE ASSOCIATIONS

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. More than 2,000 public power systems provide over 15 percent of all kilowatt-hours sales to ultimate customers and serve over 49 million people, doing business in every state except Hawaii. Over 250 public power utilities are registered entities subject to compliance with mandatory NERC Reliability Standards.

LPPC is the association of the 27 largest state-owned and municipal utilities in the nation. LPPC's members are located throughout the nation, both within and outside the boundaries of regional transmission organizations and independent system operators. The members comprise the larger, asset-owning utilities in the public power community, owning approximately 90 percent of the transmission assets owned by non-federal public power entities. LPPC members are also members of APPA.

NRECA is the national trade association representing nearly 900 local electric cooperatives and other rural electric utilities. America's electric cooperatives are owned by the people that they serve and comprise a unique sector of the electric industry. From growing regions to remote farming communities, electric cooperatives power 1 in 8 Americans and serve as engines of economic development for 42 million Americans across 56 percent of the nation's landscape.

Electric cooperatives operate at cost and without a profit incentive. NRECA's member cooperatives include 62 generation and transmission ("G&T") cooperatives and 831 distribution

cooperatives. The G&Ts generate and transmit power to distribution cooperatives that provide it to the end of line co-op consumer-members. Collectively, cooperative G&Ts generate and transmit power to nearly 80 percent of the distribution cooperatives in the nation. The remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives share an obligation to serve their members by providing safe, reliable, and affordable electric service.

UTC is the international trade association for the telecom and information technology interests of electric, gas and water utilities and other critical infrastructure industries. UTC's members include large investor-owned utilities as well as smaller rural electric cooperatives and public power providers. All types of utilities rely on private internal communications networks that utilities own and operate to support the safe, reliable and secure delivery of essential energy and water services. Many of UTC's members are subject to mandatory NERC Reliability Standards, and UTC has participated in various FERC proceedings involving reliability and cybersecurity.

III. COMMENTS

A. Information on The Extent of Use of Equipment and Services from Covered Companies

The NOI asks about the extent of the use of equipment and services provided by Covered Companies, as well as the methods used to identify such equipment and any complications associated with implementing those methods.[6] At this juncture, the Joint Trade Associations believe that the most comprehensive source of information concerning the extent to which equipment and services provided by the Covered Companies are presently used in BES operations is likely to be the response to NERC's July 8, 2020 Level 2 Alert associated with

[6] NOI at P 20.

Executive Order 13920.[7] It is Joint Trade Associations' understanding that NERC has provided the Commission with a report concerning the responses to the Alert.

Joint Trade Associations also note that NERC issued a Level 2 Alert in July 2019 based on information in the National Defense Authorization Act ("NDAA") for Fiscal Year 2019. The purpose of the Alert was "to raise awareness among NERC registered entities of persistent supply chain risks related to certain Chinese manufacturers and to request information to assess the extent of exposure of the BPS to these risks."[8] NERC reported that "[a]nalysis of the responses suggest minimal exposure of the BPS through branded products from the named Chinese telecommunications and video surveillance manufacturers and a somewhat more common use of Chinese manufactured or supplied unmanned aerial systems (UASs) for maintenance or asset management activities."[9]

As the Commission notes in the NOI, Covered Companies components also may be integrated into equipment sold by third-party vendors,[10] and this equipment is often owned and operated by telecommunications providers. The Commission and NERC have provided guidance on how to identify this equipment,[11] and Joint Trade Associations' understanding is that utility efforts in this regard are ongoing. Performing chip checks and coordinating with telecommunication service providers about equipment, however, takes time, and vendor agreements regarding the voiding of warranties may prevent thorough device testing by electric utilities independently.

---

[7] *Securing the United States Bulk-Power System*, 85 Fed. Reg. 26,595 (May 4, 2020).

[8] NERC 2020 State of Reliability Report at 4 (July 2020).

[9] *Id.*

[10] NOI at P 17.

[11] *See* FERC and NERC, *Joint Staff White Paper on Supply Chain Vendor Identification - Noninvasive Network Interface Controller* (July 31, 2020).

B. Potential Risks and Mitigation Relating to Covered Companies Equipment and Services

The Commission asks a series of questions concerning the risks to BES reliability and security posed by the use of equipment and services provided by Covered Companies, and the controls in place to prevent, detect, and mitigate the results of compromised equipment.[12] In addressing these questions, it is important to draw a distinction between risks presented by Covered Companies products that are already used in connection with the operation of the BES (including in operations planning and in business networks), and the ongoing risk presented by Covered Companies continuing to supply products and services used in connection with BES operations.

Joint Trade Associations believe that any ongoing risk associated with future procurement of Covered Companies equipment and services has already been at least partially mitigated by federal action and information alerting the industry to the potential risks associated with using such equipment or services. As noted in the NOI, for example the NDAA for 2018 included a ban on the Department of Defense using telecommunications equipment or services produced or provided by Huawei or ZTE for certain critical programs,[13] and the 2019 NDAA further expanded such restrictions.[14] The Federal Communications Commission ("FCC") has also acted, banning the use of universal service support to purchase or obtain any equipment or services produced or provided by Huawei or ZTE.[15] These actions, along with executive orders and other federal government

[12] NOI at P 20.

[13] *See* NOI at P 10 (citing National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1656 (2017)).

[14] *See id.* at P 11 (citing John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018)).

[15] *See id.* at P 12 (citing *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order (Jun. 30, 2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order (Jun. 30, 2020)).

actions described in the NOI, have sharply attuned the electric and telecommunications industries to concerns about use of Covered Companies equipment and services, and thereby helped mitigate any risks associated with future supply of such equipment and services.

As to the risks associated with Covered Companies products that are already used in connection with the operation of the BES, Joint Trade Associations emphasize that the best source of such information is likely to be federal intelligence and law enforcement authorities, on whom electric utilities must ultimately rely for timely and actionable information about the potential risks of equipment with foreign ownership, control, or influence. Joint Trade Associations' utility members could have stronger and more focused controls in place to protect assets and services from Covered Companies if improved timely and actionable information from federal authorities regarding equipment that raises foreign ownership, control, and influence concerns has been shared with utilities. Documents such as the Office of the Director of National Intelligence Report and the 2018 National Cyber Strategy of the United States of America cited in the Department of Energy's recent request for information in response to Executive Order 13920 are informative but lack actionable specifics that utility security practitioners can put to use.[16] No electric utility – regardless of size or ownership – has the expertise and capacity to evaluate foreign ownership, control, and influence concerns for all of its equipment and subcomponents. Electric utilities depend on the intelligence capabilities of the federal government to signal when a particular country or company presents an unacceptable risk to national security.

Nonetheless, as discussed below, Joint Trade Associations member utilities may employ a number of approaches, and also rely on broader industry efforts to minimize the risk of, and mitigate the impacts from, any compromise of Covered Companies equipment.

[16] *See Securing the United States Bulk-Power System*, 85 Fed. Reg. 41,023 (July 8, 2020).

C. Adequacy of the CIP Standards and Other Potential Commission Actions

The NOI asks about the effectiveness of the current CIP standards in mitigating the risks posed by equipment and services provided by Covered Companies, and seeks input on potential modifications to the CIP standards and/or other methods the Commission could employ to address these risks.[17] As discussed below, the current CIP Reliability Standards – including standards that have been approved but have not yet become effective – provide baseline security to help guard against the risks posed by Covered Companies equipment and services. Joint Trade Associations caution the Commission against adopting additional or revised mandatory standards in an effort to mitigate these risks, as this effort is unnecessary and could be counterproductive. The Commission should focus instead on facilitating information sharing by federal authorities to alert electric utilities and other stakeholders to the risks posed by Covered Companies equipment.

1. Current NERC Standards Provide an Appropriate Baseline for Protecting Against Risks from Covered Companies Equipment and Services

Nearly all the CIP standards include security controls that may assist in detecting, deterring, and mitigating the risk of cyberattack, whatever the potential attack vector, and, as such, the CIP standards provide a baseline level of security that helps guard against the risks associated with Covered Companies equipment.[18] Reliability Standard CIP-013-1 is one standard that is particularly relevant to addressing risks posed by Covered Companies equipment. Requirement 1.2.5 of CIP-013, for example, requires a process to verify software integrity and authenticity of all software and patches provided by vendors for use in BES Cyber Systems.

---

[17] NOI at P 20.

[18] While certain of the CIP standards apply only to high and medium impact BES Cyber Systems, NERC's risk-based categorization of assets appropriately calls for responsible entities to emphasize security measures for asserts that pose the greatest risk to the BES. Joint Trade Associations also note that NERC Project 2020-03 is considering future standards revisions to address supply chain risks for low impact BES Cyber Systems.

The CIP Standards also currently include requirements for incident response and reporting to the Electricity Information Sharing and Analysis Center ("E-ISAC"). CIP-008-6, R4 (future enforceable date January 1, 2021) will serve to improve those requirements, requiring responsible entities to notify the E-ISAC and the National Cybersecurity and Communications Integration Center ("NCCIC") of a Reportable Cyber Security Incident. These information sharing provisions will better posture the industry to grapple with cyber risks. Table R4 of the requirement specifies that initial notifications and updates shall include the functional impact of the incident, the attack vector used, and the level of intrusion that was achieved or attempted.[19] The industry also relies upon the Electricity Subsector Coordinating Council ("ESCC") to provide an avenue for public-private coordination from a national level. The ESCC provides strategic leadership for all hazards to the grid, which includes cyberattack.

Other CIP standards that particularly address risks associated with Covered Companies equipment include CIP-005-6, which requires utilities to manage electronic access to high and medium impact BES Cyber Systems, including system-to-system remote access. Under the standard, responsible entities must have the capability to disable active remote access sessions, including system-to-system sessions, in the event of a system breach. Reliability Standard CIP-007-6 requires responsible entities to manage system security, and CIP-010-3 addresses prevention and detection of unauthorized changes to high and medium impact BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements to protect BES assets from compromise that could lead to misoperation or instability in the BES.

[19] Additionally, NERC Standard EOP-004-4, R2 states that entities must promptly report BES events to the ERO and other specified entities, regardless of the initiating cause.

In addition to the CIP standards, EOP-004-4 requires that responsible entities have an event reporting Operating Plan in accordance with EOP-004-4, Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations. Attachment 1 lists several event types that are required to be covered, all of which could result from a cyberattack in theory. Recovery from physical and cyber events is addressed by standard EOP-005.

Registered entities, moreover, have implemented varied security controls that likely would help minimize risks associated with Covered Companies equipment, including:

- Using utility-owned and operated communication paths for critical operations traffic to minimize the risk of internet or local TELCO circuit disruptions affecting those communications.
- Implementing network separation and isolation techniques that do not allow communications between asset locations to mitigate the effects of a potential cyberattack.
- Following the requirements of EOP-008-3 that require a back-up control center to mitigate the possibility of the same threat affecting both locations.

In addition to these controls, the fact that registered entities use different and diverse equipment sets, as well as varied techniques to isolate that equipment from cyberattack provides some mitigation of the risk of a cyberattack associated with Covered Companies equipment and services. Finally, for those utilities that do not have BPS assets, cyber and physical security best practices, maturity models, and frameworks that include remote monitoring and management are widely utilized.

2. Additional CIP Standards or Requirements

Joint Trade Associations believe that the existing CIP standards, in conjunction with other activities aimed at pursuing a defense in depth strategy toward cybersecurity, substantially mitigate the risks to the BES posed by Covered Companies equipment and services. Joint Trade

Associations caution the Commission against adopting additional or revised mandatory standards in an effort to mitigate these risks, as this effort is unnecessary and could be counterproductive.

Electric utilities use various approaches to provide telecommunications services on their systems, and there is unlikely to be a "one size fits all" approach to addressing these risks. For public power and cooperative utilities in particular, the wide variation in their sizes, facilities, and system topologies makes for a wide variation in the security protocols they require and use to adequately protect their systems. Joint Trade Associations believe that the key to effective additional security measures will be a strategic, risk-based approach, focused on the most critical resources and highest priority threats. If the number of entities impacted by Covered Companies equipment is relatively limited, this would mitigate the need for mandatory, industry-wide standards or requirements.

With the continued sophistication of cyberattacks, having today's flexible logic-based CIP standards provides the best framework to keep pace with threats posed by equipment and services provided by the Covered Companies and other foreign ownership, control, and influence concerns.

It is also important to emphasize that the risks posed by Covered Companies equipment is not limited to the electric sector subject to a mandatory reliability standard framework. Covered Companies components may be integrated into equipment sold by third-party vendors, and this equipment is often owned and operated by telecommunications providers. Indirectly imposing obligations on telecommunications providers through new or revised mandatory CIP standards could conflict with telecommunication mandates or protocols. Demands by electric utilities that telecommunications providers conform to requirements imposed on the utilities by new CIP standards or requirements could also potentially reduce the willingness of telecommunications providers to serve electric utilities, which in Joint Trade Associations' experience, the providers

view as a relatively unattractive, low-margin service in the first place.

Joint Trade Associations would also be concerned with any standards or requirements that could require removal and replacement of existing equipment in a manner that could expose responsible entities to prohibitive costs or supply shortages, particularly in the absence of clear guidance that such steps are essential to securing the BPS. Existing equipment should not be required to be removed until there are sufficient mitigation measures to eliminate and reduce known risks.

3. The Commission Should Facilitate Information Sharing

Rather than consider additional CIP standards or requirements to address potential risks posed by equipment and services provided by Covered Companies (and other entities that may pose a threat to national security), the Commission should focus its efforts on facilitating information sharing. Having the proper security controls in place to identify, mitigate, and protect against cyberattacks relies on utilities obtaining timely and actionable information from their government partners. The federal government can continue to improve security related information exchanges by allowing for timely and actionable sharing of threats, including immediate actions that a utility should take to mitigate risks. Additionally, expeditiously declassifying this information is extremely critical so that energy sector entities that are not clearance holders can take appropriate mitigation measures. Joint Trade Associations encourage the Commission to promote such information sharing policies and protocols.

Joint Trade Associations are not recommending that information sharing protocols be added to the CIP standards to the extent that they are not already included. We note that additional information sharing between local and regional entities would always provide enhanced awareness of situations that could benefit proximate entities. In general, however, these communications

occur already under existing mechanisms and adding additional regulatory requirements would not necessarily enhance the quality or frequency. Joint Trade Associations look forward to further discussion of coordinated measures that may be taken on a regional or national basis.

IV. CONCLUSION

Joint Trade Associations appreciate the opportunity to comment on the NOI, and we look forward to working with the Commission as its consideration of these issues proceeds.

Respectfully submitted,

American Public Power Association

/s/ John E. McCaffrey
John E. McCaffrey
Senior Regulatory Counsel
Jack Cashin
Director, 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

National Rural Electric Cooperative Association

/s/ Barry R. Lawson
Barry R. Lawson
Senior Director, Regulatory Affairs
National Rural Electric Cooperative Association
4301 Wilson Blvd
11th Floor
Arlington, VA 22203
703-907-5781
Barry.lawson@nreca.coop

Large Public Power Council

/s/ Jonathan D. Schneider
Jonathan D. Schneider
Jonathan P. Trotta
Stinson LLP
1775 Pennsylvania Avenue NW
Suite 800
Washington, DC 20006
(202) 728-3034
jonathan.schneider@stinson.com
jtrotta@stinson.com

Utilities Technology Council

/s/ Brett Kilbourne
Brett Kilbourne
Vice President Policy and General Counsel
Utilities Technology Council
2550 South Clark Street, Suite 960
Arlington, VA 22202
202-872-0030
Brett.kilbourne@utc.org

November 23, 2020