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**

INITIAL COMMENTS OF THE UNITED STATES DEPARTMENT OF ENERGY

The United States Department of Energy ("DOE") files these initial comments with the Federal Energy Regulatory Commission ("FERC" or the "Commission") in response to the Commission's Notice of Inquiry ("NOI") dated September 17, 2020 seeking comments on the potential risks to the bulk electric system posed by using equipment and services produced or provided by entities identified as risks to national security.[1]

I. Background

A. 2019 NDAA

In the NOI, the Commission has focused on those corporations that were identified in section 889(f)(3) of the National Defense Authorization Act for Fiscal Year 2019,[2] and specifically Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, and any subsidiary or affiliate of such entities, as well as any other 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.[3] These entities are referred to by the Commission in the NOI as "Covered

[1] Notice of Inquiry, *Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security*, FERC Docket No. RM20-19-000, 172 FERC ¶ 61,224 (Sept. 17, 2020).
[2] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3)(2018) ("2019 NDAA").
[3] NOI at P 19.

Companies." As set forth in the 2019 NDAA, Congress prohibited executive agencies from contracting with the Covered Companies for telecommunications and video surveillance equipment and services.[4]

B. Executive Order 13873

On May 15, 2019, the President issued Executive Order 13873 on "Securing the Information and Communications Technology and Services Supply Chain."[5] Executive Order 13873 declared a national emergency based on a finding that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services." To address this risk, Executive Order 13873 directs the Secretary of Commerce, in consultation with other agency heads, to identify any acquisition, importation, transfer, installation, dealing in, or use of any information and communication technology or service where the transaction involves any property in which any foreign country or a national thereof has any interest.[6]

C. Executive Order 13920

On May 1, 2020, the President issued Executive Order 13920 declaring "a national emergency with respect to the threat to the United States bulk-power system" as a result of the threat to national security, foreign policy, and the economy of the United States presented by the unrestricted foreign supply of bulk-power system electric equipment.[7] Executive Order 13920 prohibits the acquisition, importation, transfer, or installation of any bulk-power system electric equipment (a "transaction") where the transaction was initiated after May 1, 2020, and where the

[4] 2019 NDAA, § 889(a).
[5] Executive Order No. 13873, 84 FR 22689 (May 17, 2019). On May 13, 2020, the President continued for one year the national emergency declared in Executive Order 13873. Notice on the Continuation of the National Emergency on Securing the Information and Communications Technology and Services Supply Chain. 85 FR 29321 (May 14, 2020).
[6] 84 FR at 22689.
[7] Executive Order No. 13920, 85 FR 26595 (May 4, 2020).

Secretary, in coordination with the Director of the Office of Management and Budget and in consultation with the heads of other relevant agencies, has determined that:

(a) the transaction involves bulk-power system electric equipment designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(b) the transaction:

(i) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of the bulk-power system in the United States;

(ii) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States; or

(iii) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

Executive Order 13920 authorizes the Secretary of Energy to take action as appropriate and consistent with applicable law to implement the Executive Order, including by order and rulemaking.[8]

D. The Commission's Notice of Inquiry

In the NOI, following a review of the 2019 NDAA, Executive Order 13873 and Executive Order 13920, the Commission poses for comment five principal questions related to the Covered Companies: (1) the extent to which equipment and services provided by Covered Companies are used in the operation of the bulk electric system; (2) the risks posed to bulk electric system

[8] 85 FR at 26596. DOE maintains a website with information related to Executive Order No. 13920 at https://www.energy.gov/oe/bulkpowersystemexecutiveorder. This website is updated as implementation activities proceed.

reliability and security by the use of equipment and services provided by Covered Companies; (3) the effectiveness of current Critical Infrastructure Protection (CIP) Reliability Standards[9] in mitigating the risks posed by equipment and services provided by Covered Companies and used in the operation of the bulk electric system; (4) strategies that entities have implemented or plan to implement to mitigate the risks associated with use of equipment and services provided by Covered Companies; and (5) other methods that the Commission could employ outside of the CIP Reliability Standards to further address the risk to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies.[10]

II. Comments of the Department of Energy

A. The Commission Should Address the Threat Posed by the Covered Companies

The Covered Companies (Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company) clearly pose a threat to the bulk electric system. Congress in the 2019 NDAA prohibited executive agencies from contracting with the Covered Companies for telecommunications and video surveillance equipment and services. Moreover, the Covered Companies' telecommunications and video surveillance equipment and services should not be used in the bulk electric system. As suggested by the Commission in the NOI, the CIP Reliability Standards provide a mechanism to develop rules and procedures to prohibit participation by the Covered Companies in the bulk electric system supply chain.

[9] *See* NOI at P 2, n.1 (citing Reliability Standards CIP-013-1 (Cyber Security – Supply Chain Risk Management), CIP-005-6 (Cyber Security – Electronic Security Perimeter(s)), and CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments). *Supply Chain Risk Management Reliability Standards*, Order No. 850, 165 FERC ¶ 61,020 (2018)).

[10] NOI at P 20.

B. CIP Reliability Standards and Other Industry Standards and Practices Should Address the Risks to the Bulk Electric System Posed by Identified Foreign Adversaries

The Commission should direct the North American Electric Reliability Corporation (NERC) to initiate an examination of the CIP Reliability Standards to identify any gaps in application to address the risks to the bulk electric system posed by foreign adversaries. This issue goes beyond the narrow confines of the Covered Companies (and the telecommunications and video surveillance equipment and services that those companies supply) addressed in the NOI and extends to the electric equipment comprising the bulk electric system. Rather than creating another layer of practices and standards, DOE supports clarification or modification of CIP Reliability Standards as may be necessary to explicitly recognize and address foreign adversary risks at each tier of the supply chain, including materials sourcing, manufacturing, assembling, procurement, delivery, and installation, as well as operation and monitoring.

On July 8, 2020, DOE published a Request for Information in connection with its efforts under Executive Order 13920 in which it sought public comment on the energy industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system.[11] As explained in its Request for Information,

> The Department will build upon efforts by standards development organizations, including but not limited to, NIST 800 series standards (see *https://csrc.nist.gov/publications/sp800*), ISO standards (see *https://www.iso.org/home.html*), ISA/IEC 62433 standards (see *http://www.isa.org/intech/201810standards/*), and NERC–CIP standards (see *https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx*).[12]

In response to the Request for Information, DOE received 98 responses from a broad range of parties active in the electricity sector.[13] DOE continues to review and analyze those comments

[11] 85 FR 41023 (July 8, 2020).
[12] 85 FR at 41024.
[13] The responses can be seen at https://www.regulations.gov/document?D=DOE-HQ-2020-0028-0001.

and to develop further action reflecting those comments, where appropriate. However, it is clear from the responses that many commenters advocate for building on existing standards and practices rather than creating a new supply chain risk management structure. At the same time, a number of commenters share the view that existing standards and practices do not adequately address the risk to the bulk electric system supply chain of foreign adversaries.

Thus, DOE recommends that the Commission examine how the CIP Reliability Standards could more clearly address foreign risk and look beyond just the Covered Companies, in coordination with DOE's initiatives to implement Executive Order 13920. For example, DOE is not considering developing a separate supply chain risk management tool, but intends to focus on improving utility owner/operator's asset and operations risk assessments through the incorporation of enterprise risk posed by foreign adversaries.[14] In addition, DOE may consider integrating new supply chain criteria in future DOE procurements related to the bulk-power system. DOE encourages bulk-power system owners and operators to comprehensively and objectively assess, to the extent possible, the following criteria:

1. Whether the supplier is headquartered in a country where the laws and policies governing manufacturers are guided by the demonstrable respect for the rule of law, shown by clear legal or judicial limitations on the exercise of power by the government to own, control, or influence product development and data handling. Suppliers with an opaque ownership structure and financial structure, which are state-owned and disguise or obscure who owns, controls, or influences the company and its interactions would be considered less trustworthy. Suppliers are less trustworthy if the national laws of the country where they are headquartered mandate cooperation with

[14] 85 FR at 41024.

the government or give the government special rights that cannot be challenged in court, the national legislature, or another domestic institution.

2. Whether the supplier can present credible third-party assessments and certify that the technology and software code has been designed and developed to internationally- or nationally-recognized standards. The supplier's ability to provide assurances on the pedigree of its subcomponents and third-party software, including provenance and software bill of materials, would demonstrate greater trustworthiness.

3. Whether the supplier has implemented verifiable technical measures to ensure the application of strict access controls to authorized users in product development, business operations, and network operations.

DOE also recognizes other guidance and criteria that are also available to help entities assess supply chain risk.[15]

Existing standards and practices can additionally be improved through (i) the use of machine learning, artificial intelligence, and other developments that increase the speed and efficiency of risk assessment, and (ii) increased communication among stakeholders regarding foreign adversary risk and mitigation, not only through Commission and NERC processes, but also the Electricity Subsector Coordinating Council and information sharing through the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the Electricity

[15] *See e.g.*, Center for Strategic and International Studies, Criteria for Security and Trust in Telecommunications Networks and Services (May 2020), https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services; North American Electric Reliability Corporation, *Cyber Security Supply Chain Risk Management Plans: Implementation Guidance for CIP-013-2* (Apr. 2017), https://www.nerc.com/pa/Stand/Project%20201603%20Cyber%20Security%20Supply%20Chain%20Managem/Implementation_Guidance_071117.pdf; and Edison Electric Institute, *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk* (May 2020), https://www.eei.org/issuesandpolicy/Documents/EEI%20Law%20-%20Model%20Procurement%20Contract%20Language.pdf.

Information Sharing and Analysis Center, and DOE's Office of Cybersecurity, Energy Security, and Emergency Response.

Furthermore, in its Request for Information, DOE explained that the current list of foreign adversaries for purposes of Executive Order 13920 consists of the People's Republic of China (China), the Republic of Cuba (Cuba), the Islamic Republic of Iran (Iran), the Democratic People's Republic of Korea (North Korea), the Russian Federation (Russia), and the Bolivarian Republic of Venezuela (Venezuela).[16] While the participation in the bulk electric system supply chain of persons that are potentially owned, controlled, influenced by each of the foreign adversaries ranges from extensive (e.g., China) to little current activity, DOE's identification of these nation states as foreign adversaries for purposes of Executive Order 13920 is important in scoping supply chain management practices and assessing the risks presented by each particular foreign adversary. DOE's explanation of the basis for this determination also provides information regarding how foreign adversaries will be identified, insofar as global dynamics are likely to remain in flux, and the identification of foreign adversaries with respect to the bulk electric system may be amended as circumstances warrant.[17]

Finally, DOE offers a comment on the use of incentives to implement foreign adversary risk assessment in supply chain risk management. As DOE noted in its comments on the Commission staff's Cybersecurity Incentives White Paper,[18] DOE supports incentives that accelerate the development and deployment of technologies that "increase national security by helping to prevent or minimize adverse impacts to energy infrastructure systems," and in that case specifically high-fidelity sensor-based continuous network monitoring cybersecurity capabilities

[16] 85 FR at 41024.
[17] *Id*.
[18] Cybersecurity Incentives White Paper, FERC Docket No. AD20-19-000 (June 18, 2020).

for operating the transmission system (e.g., operational technology).[19] Similarly, supply chain management measures adopted to address foreign adversary risk may also merit incentive treatment. Nevertheless, in the case of the Covered Companies that are the subject of the NOI, DOE does not see a basis to award incentives to energy sector stakeholders to adopt prohibitions similar to those set forth in the 2019 NDAA. The identity of the Covered Companies and the risks posed by those companies and the products and services they supply have been widely identified, including in the 2019 NDAA, and the energy sector should be taking steps to eliminate those companies from their supply chains.

DOE appreciates the opportunity to submit these initial comments in response to the NOI and looks forward to partnering with FERC on this important endeavor.

Respectfully submitted,

/s/ Patricia A. Hoffman
Patricia A. Hoffman
Acting Assistant Secretary
Office of Electricity
United States Department of Energy

/s/ Nicholas Andersen
Nicholas Andersen
Principal Deputy Assistant Secretary
Office of Cybersecurity, Energy Security, and Emergency Response
United States Department of Energy

Dated: November 20, 2020

[19] Reply Comments of the United States Department of Energy, Docket No. AD20-19-000 (Aug. 28, 2020).