172 FERC ¶ 61,224
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

[Docket No. RM20-19-000]

Equipment and Services Produced or Provided by Certain Entities Identified as Risks to National Security

(September 17, 2020)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Inquiry.

SUMMARY: The Federal Energy Regulatory Commission (Commission) seeks comments on the potential risks to the bulk electric system posed by the use of equipment and services produced or provided by certain entities identified as risks to national security. In addition, the Commission seeks comments on strategies to mitigate any potential risks posed by such telecommunications equipment and services, including but not limited to potential modifications to the Critical Infrastructure Protection Reliability Standards.

DATES: Initial Comments are due **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and Reply Comments are due **[INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.
- Mail/Hand Delivery: Those unable to file electronically may mail or hand-deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.
- *Instructions*: For detailed instructions on submitting comments, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

Simon Slobodnik (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6707
Simon.Slobodnik@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
Kevin.Ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

172 FERC ¶ 61,224
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF INQUIRY

(September 17, 2020)

1. In this Notice of Inquiry, the Commission seeks 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. In addition, the Commission seeks comments on whether the current Critical Infrastructure Protection (CIP) Reliability Standards adequately mitigate the identified risks. Further, the Commission seeks comment on possible actions the Commission could consider taking to address the identified risks.

2. On October 18, 2018, the Commission approved the first set of supply chain risk management Reliability Standards in Order No. 850.[1] The Commission described the supply chain risk management Reliability Standards as "forward-looking and objective-

[1] The Commission approved 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).

based and require each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations."[2] In approving the supply chain risk management Reliability Standards, the Commission recognized that "the global supply chain creates opportunities for adversaries to directly or indirectly affect the management or operations of companies with potential risks to end users."[3]

3. Since the issuance of Order No. 850, there have been significant developments in the form of Executive Orders, legislation, as well as federal agency actions that raise concerns over the potential risks posed by the use of equipment and services provided by certain entities identified as risks to national security. In particular, Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) have been identified as examples of such certain entities because they provide communication systems and other equipment and services that are critical to bulk electric system reliability.[4]

4. Therefore, as discussed in this Notice of Inquiry, the Commission seeks comments on: (1) the extent of the use of equipment and services provided by certain entities identified as risks to national security related to bulk electric system operations; (2) the risks to bulk electric system reliability and security posed by the use of equipment and

[2] *Id.* P 2.

[3] *Id.*

[4] *See e.g.* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(f)(3) (2018) (2019 NDAA).

services provided by certain entities; (3) whether the CIP Reliability Standards adequately mitigate the identified risks; (4) what mandatory actions the Commission could consider taking to mitigate the risk of equipment and services provided by certain entities related to bulk electric system operations; (5) strategies that entities have implemented or plan to implement – in addition to compliance with the mandatory CIP Reliability Standards – to mitigate the risks associated with use of equipment and services provided by certain entities; and (6) other methods the Commission may employ to address this matter including working collaboratively with industry to raise awareness about the identified risks and assisting with mitigating actions (i.e., such as facilitating information sharing). The responses to these questions will provide the Commission with a better understanding of the risks to bulk electric system reliability posed by equipment and services provided by entities identified as risks to national security, as well as how the Commission may best address any identified risks.

I. Background

A. Executive Orders on Bulk-Power System Security

5. On May 15, 2019, President Trump issued Executive Order 13,873 on "Securing the Information and Communications Technology and Services Supply Chain."[5] Executive Order 13,873 declared a national emergency based on a finding that:

> foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services … in order to commit malicious

[5] Executive Order No. 13,873, 84 FR 22689 (May 17, 2019).

> cyber-enabled actions, including economic and industrial espionage against the United States and its people.

To address that risk, Executive Order 13,873 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 communications technology or service . . . where the transaction involves any property in which any foreign country or a national thereof has any interest."

6. Executive Order 13,873 directs the Secretary of Commerce, in consultation with other agency heads, to identify such prohibited transactions by determining whether: (1) the transaction involves information and communications technology or services designed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and (2) the transaction poses an undue risk of sabotage to or subversion of the design or operation of information and communications technology or services in the United States or poses an undue risk of catastrophic effects on the security of United States critical infrastructure.

7. On May 1, 2020, President Trump issued Executive Order 13,920 on "Securing the U.S. Bulk-Power System," declaring a national emergency based on the findings that "foreign adversaries are increasingly creating and exploiting vulnerabilities" in the Bulk-Power System and that the "unrestricted foreign supply of bulk-power system electric equipment constitutes an unusual and extraordinary threat to the national security." [6]

[6] Executive Order No. 13,920, 85 FR 26595 (May 4, 2020).

8. To address these risks, Executive Order 13,920 prohibits the acquisition, importation, transfer, or installation of any Bulk-Power System electric equipment where the transaction: (1) involves Bulk-Power System electric equipment designed, developed, manufactured, or supplied, by a foreign adversary; and (2) the transaction poses an undue risk of sabotage to the Bulk-Power System or poses an undue risk to U.S. critical infrastructure, economy or national security. In addition, Executive Order 13,920 establishes a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security (Task Force), chaired by the Secretary of Energy.[7] The Task Force is directed to: (1) develop energy infrastructure procurement policies for agencies; (2) evaluate methods to incorporate national security considerations into energy security and cybersecurity policymaking; (3) consult with the Electric Subsector Coordinating Council (and the oil and natural gas sector equivalent) in developing recommendations; and (4) conduct other studies and develop other recommendations as appropriate.

B. National Defense Authorization Acts

9. Recently, Congress has addressed the risks posed by the procurement of equipment and services from entities identified as risks to national security in the annual National Defense Authorization Acts.

[7] The Secretary of Energy has until September 28, 2020, to promulgate the necessary regulations. *See* Dept. of Energy, Request for Information, 85 FR 41023 (July 8, 2020) (the public comment period is open until Aug. 24, 2020).

10. The National Defense Authorization Act for Fiscal Year 2018 bars the Department of Defense from using "[t]elecommunications equipment [or] services produced [or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.[8]

11. In addition, the National Defense Authorization Act for Fiscal Year 2019 prohibits the Secretary of Defense from procuring or obtaining, or extending or renewing a contract to procure or obtain, equipment, systems, or services that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system. Specifically, section 889(f)(3) of the 2019 NDAA defines "covered telecommunications equipment or services" as:

> (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced or provided by 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.[9]

---

[8] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1656 (2017) (2018 NDAA).

[9] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub.

C. Federal Communication Commission Orders on Communications Supply Chain

12. On June 30, 2020, the Federal Communications Commission (FCC) issued two orders designating both Huawei and ZTE as covered entities that are prohibited from receiving Universal Service Fund moneys to support the purchase of any equipment or services provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.[10] The FCC Orders determined that Huawei and ZTE pose a national security threat to the integrity of communications networks and the communications supply chain due to their close ties to the Chinese government. The FCC found that Huawei is susceptible to coercion, both legal and political, presenting profound risks to the security of affected communications networks. The FCC also found that Huawei's close ties to the Chinese government, both at the level of ownership and at the employee level, as well as its obligations under Chinese law, present too great a risk to U.S. national security to continue to subsidize the use of Huawei equipment and services.

13. Likewise, with respect to ZTE, the FCC noted the company's obligations under Chinese law to permit Chinese government entities, including state intelligence agencies,

---

L. No. 115-232, § 889(f)(3) (2018) (2019 NDAA).

[10] *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).

to demand that private communications sector entities cooperate with governmental requests, including revealing customer information and network traffic information. The FCC also found that security risks and vulnerabilities in ZTE's equipment pose a threat to the integrity of communications networks and the communications supply chain. The FCC, furthermore, identified various reports that identify a wide range of vulnerabilities and cybersecurity risks found in ZTE equipment, which have led to an increase in restrictions placed upon its availability in the U.S. market.

D. The 5G Ecosystem: Risks and Opportunities for the Department of Defense

14. A report by the Defense Innovation Board, titled "The 5G Ecosystem: Risks and Opportunities for DoD," highlights the threats posed by China and other nation-state adversaries.[11] The report notes that "evidence of backdoors or security vulnerabilities have been discovered in a variety of devices globally" and that many of those vulnerabilities "seem to be related to requirements from the Chinese intelligence community pressuring companies to exfiltrate information."[12] The report also highlights the need for the Department of Defense to "consider options for defending against a

[11] The 5G Ecosystem: Risks and Opportunities for DoD, Defense Innovation Board (Apr. 3, 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[12] *Id.* at 25.

compromised supply chain, where Chinese semiconductor components and chipsets are embedded across multiple systems."[13]

II. Discussion

A. Analysis

15. Recent Executive Orders, legislation and federal agency decisions have identified Huawei and ZTE, as well as other entities identified as risks to national security, as potential risks to national security. The FCC has gone so far as to designate both Huawei and ZTE as national security threats to the integrity of communications networks and the communications supply chain. These actions raise concerns over the potential risks to bulk electric system reliability posed by the use of equipment and services provided by Huawei, ZTE, and other entities identified as risks to national security.

16. The Commission has previously noted that responsible entities such as reliability coordinators, balancing authorities, and transmission operators must be capable of receiving and storing a variety of sensitive bulk electric system data from interconnected entities in order to adequately perform their reliability functions.[14] The critical role played by communications networks in maintaining bulk electric system reliability by, among other things, helping to maintain situational awareness and reliable bulk electric system operations through timely and accurate measurement, collection, processing of

[13] *Id.* at 29.

[14] *See Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, at P 54, *order denying reh'g*, Order No. 822-A, 156 FERC ¶ 61,052 (2016).

bulk electric system status and information exchange among control centers makes it necessary for the Commission to understand the risk to bulk electric system reliability posed by the use of equipment and services provided by Huawei, ZTE, and other entities identified as risks to national security.

17. There are many manufacturers of networking and telecommunications equipment, but Huawei, ZTE, and their subsidiaries are gaining substantial shares of the market globally.[15] A portion of this exposure to Huawei and ZTE stems from embedded Huawei or ZTE components in equipment produced by unaffiliated vendors. The probability that electric utilities now use a significant amount of telecommunications equipment with embedded components from Huawei or ZTE is greater in consideration of these facts, especially when factoring in components that are branded under a different vendor's label. If these obscured, or potentially unlabeled, components are present in an electric utility's infrastructure, the same risks may exist as if the hardware had been purchased directly from Huawei, ZTE, or one of their subsidiaries.

18. In addition, the Commission notes that Executive Order No. 13,920 on Securing the U.S. Bulk-Power System includes a definition for "bulk-power system electric equipment" that covers a range of electrical equipment commonly used in substations,

[15] *See, e.g., Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong., at 2 (Oct. 8, 2012) (finding "Chinese telecommunications firms, such as Huawei and ZTE, are rapidly becoming dominant global players in the telecommunications market").

generating stations, and control rooms.[16] Huawei or ZTE equipment or components that fall within these categories may also raise concerns over the potential risks to bulk electric system reliability posed by their use.

B. Request for Comments

19. The Commission seeks comment on the potential risk to bulk electric system reliability posed by the use of equipment and services provided by entities identified in section 889(f)(3) of the 2019 NDAA (Covered Companies).[17]

20. Below, we pose questions that commenters should address in their submissions. However, commenters need not address every topic or answer every question identified below. Please do not include confidential or proprietary information, CEII, or other sensitive or classified information in your responses.

Q1. To what extent is the equipment (including components) and services provided by Covered Companies used in the operation of the bulk electric system?

a. What methods could be used to ascertain the extent to which equipment and services provided by Covered Companies is used in the operation of the bulk electric system?

b. Describe any potential complications to system operations that may result from implementing such methods (e.g., need to shut down certain activities to perform testing).

Q2. Describe the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies?

a. Describe the range of potential security impacts to bulk electric system reliability that could occur if a responsible entity uses the equipment and

---

[16] Executive Order No. 13,920 at section 4(b), 85 FR 26595 (May 4, 2020).

[17] *See supra* P 11.

services provided by the Covered Companies within its real-time operations infrastructure and the equipment was compromised.

b. If equipment and services provided by Covered Companies is installed in a responsible entity's real-time operations infrastructure, what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise?

c. Describe the range of potential security impacts to bulk electric system reliability from a compromise of a responsible entity's systems related to non-real time bulk electric system operations (e.g., operations planning) resulting from the use of equipment and services provided by Covered Companies.

d. If equipment and services provided by Covered Companies is installed in a non-real time environment (e.g. operations planning), what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise?

e. Describe the potential range of security impacts to bulk electric system reliability from a compromise of responsible entity's systems related to non-bulk electric system communications and operations (e.g., business networks and systems not directly related to bulk electric system operations) resulting from the use of equipment and services provided by Covered Companies.

f. If equipment and services provided by Covered Companies is installed in a non-bulk electric system communications and operations environment (e.g., business networks and systems not directly related to bulk electric system operations), what controls are in place to prevent or detect compromise? What controls are in place to mitigate the potential effects of compromise? What controls are in place to prevent compromise of business network or systems from migrating and impacting bulk electric system operations?

Q3. Discuss the effectiveness of the current CIP Reliability Standards in mitigating the risks posed by equipment and services provided by Covered Companies used in the operation of the bulk electric system.

a. Which requirements of the CIP Reliability Standards, including complementary requirements across the CIP Reliability Standards, require entities to take actions that detect and mitigate the risks associated with the use of equipment and services provided by Covered Companies?

b. What modifications to the CIP Standards would minimize risks associated with equipment and services provided by the Covered Companies?

Q4. Describe any strategies, in addition to compliance with the CIP Reliability Standards, entities have implemented or plan to implement to mitigate the risks associated with use of equipment and services provided by Covered Companies.

Q5. What other methods could the Commission employ outside the CIP Reliability Standards, whether through regulatory action or through voluntary collaboration with industry and government, to further address the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies? For example, raising awareness about the risks identified in response to the previous questions, identifying potential solutions, and assisting with mitigating actions (including the facilitating information sharing)?

a. Describe how your organization is informed of the risks to bulk electric system reliability and security posed by the use of equipment and services provided by Covered Companies and what could be done to improve this process.

b. What actions has your organization taken to address these risks and what impediments exist to do so (i.e., such as procurement process requirements)?

c. What challenges does your organization face when identifying, containing or removing equipment that presents supply chain threats from Covered Companies?

III. Comment Procedures

21. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**], and Reply Comments are due [**INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. Comments must refer to Docket No. RM20-19-000, and must include the commenter's name, the organization they represent, if applicable, and their address.

22. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word-processing formats. Documents created electronically using word-processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

23. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

24. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

IV. Document Availability

25. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through the Commission's Home Page (http://www.ferc.gov) and in the Commission's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. eastern time) at 888 First Street NE, Room 2A, Washington, DC 20426.

26. From the Commission's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and

Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

27. User assistance is available for eLibrary and the Commission's website during normal business hours from the Commission's Online Support at (202) 502-6652 (toll free at 1-866-208-3676) or email at ferconlinesupport@ferc.gov, or the Public Reference

Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.