[6450-01-P]

DEPARTMENT OF ENERGY

Prohibition Order Securing Critical Defense Facilities

AGENCY: Office of Electricity, Department of Energy.

ACTION: Prohibition Order.

SUMMARY: The U.S. Department of Energy (Department or DOE) gives notice of this Prohibition Order prohibiting the acquisition, importation, transfer, or installation of specified bulk-power system (BPS) electric equipment that directly serves Critical Defense Facilities (CDFs), pursuant to Executive Order 13920.

DATES: The effective date of this Prohibition Order (Effective Date) is January 16, 2021. This Prohibition Order shall apply to any Prohibited Transaction initiated on or after the Effective Date. The Department shall notify each Responsible Utility of the applicability of this Prohibition Order no later than five (5) business days after the issuance of this Prohibition Order. Notice under this section shall be deemed made when personally delivered or when mailed, three (3) calendar days after deposit in the U.S. Mail, first class postage prepaid and addressed to the Responsible Utility at its applicable address. Actual notice shall be deemed adequate notice on the date actual notice occurred, regardless of the method of service.

FOR FURTHER INFORMATION CONTACT:

Mr. Charles Kosak, Deputy Assistant Secretary, Energy Resilience Division, U.S. Department of Energy, Office of Electricity, Mailstop OE-20, Room 8G-042, 1000 Independence Avenue, SW, Washington, DC 20585; (202) 586-2036; or *bulkpowersystemEO@hq.doe.gov*.

SUPPLEMENTARY INFORMATION:

RATIONALE FOR THE ORDER:

Executive Order No. 13920 of May 1, 2020, *Securing the United States Bulk-Power System* (85 FR 26595 (May 4, 2020)) (EO 13920) declares that threats by foreign adversaries[1] to the security of the BPS constitute a national emergency. A current list of such adversaries is provided in a Request for Information (RFI), issued by the Department of Energy (Department or DOE) on July 8, 2020,[2] seeking public input to aid in its implementation of EO 13920. The Department has reason to believe, as detailed below, that the government of the People's Republic of China (PRC or China), one of the listed adversaries, is equipped and actively planning to undermine the BPS. The Department has thus determined that certain BPS electric equipment or programmable components subject to China's ownership, control, or influence, constitute undue risk to the security of the BPS and to U.S. national security. The purpose of this Order is to prohibit the acquisition, importation, transfer, or subsequent installation of such BPS electric equipment or programmable components in certain sections of the BPS.

The PRC has a military rationale for its disruption capabilities. Broadly speaking, it is targeting operational systems that can be undermined as a way to degrade an opponent's capabilities or to coerce an opponent's decision-making or political will. China calls this "system destruction warfare"—a way to cripple an opponent at the outset of conflict, by deploying sophisticated electronic warfare, counter-space, and cyber-capabilities to disrupt what are known as C4ISR networks (command, control, communications, computers, intelligence, surveillance, and

[1] Section 4(d) of EO 13920 defines "foreign adversary" to mean "any foreign government or foreign non-government person engaged in a long-term pattern of serious instances of conduct significantly adverse to the national security of the United States or its allies or the security and safety of United States persons."
[2] 85 FR 41023, *https://www.govinfo.gov/content/pkg/FR-2020-07-08/pdf/2020-14668.pdf*.

reconnaissance), thereby disrupting U.S. military logistics required to defend the homeland, support Allies and partners, and protect key U.S. national security interests.[3]

Such attacks are most likely during crises abroad where Chinese military planning envisions early cyberattacks against the electric power grids around CDFs in the U.S. to prevent the deployment of military forces and to incur domestic turmoil. Underscoring this, the Department of Defense's *2018 National Defense Strategy* assessment is that the homeland is no longer a sanctuary and that malicious cyber activity against personal, commercial, or government infrastructure is growing significantly, "while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities."[4]

U.S. intelligence analyses validate this growing threat from China, concluding that "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems," and "has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[5] Indeed, according to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, open-source reporting indicates that "offensive cyber operations attributed to the Chinese government targeted, and continue to target, a variety of industries and organizations in the United States," including energy firms.[6] The National

[3] Chairman of the Joint Chiefs of Staff Instruction, Responsibilities for the Joint Tactical Operations Interface Training Program (Aug. 13, 2012), *https://www.jcs.mil/Portals/36/Documents/Library/Instructions/6240_01.pdf*.
[4] U.S. Dep't of Defense, Summary of the 2018 National Defense Strategy of the United States of America, at 3, *https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf*.
[5] Coats, Daniel R., Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, at 5 (Jan. 29, 2019), *https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf*.
[6] U.S. Dep't of Homeland Security, Cybersecurity and Infrastructure Security Agency, "Potential for China Cyber Response to Heightened U.S.–China Tensions," Alert AA20-275A (Oct. 20, 2020), *available at https://us-cert.cisa.gov/ncas/alerts/aa20-275a*.

Security Agency has determined that "one of the greatest threats to U.S. National Security Systems, the U.S. Defense Industrial Base, and Department of Defense information networks is Chinese state-sponsored malicious cyber activity."[7]

Furthermore, China's laws, specifically the National Intelligence Law and the National Cybersecurity Law, authorize government officials to exercise control over individuals and companies to conduct national intelligence work and access private company data, which provide opportunities for China to identify and exploit vulnerabilities in Chinese-manufactured or supplied equipment that are used in U.S. critical infrastructure that rely on these sources.

For example, the National Intelligence Law compels individuals and organizations to comply with and assist PRC officials in carrying out intelligence and national security objectives. Specifically, Article 7 requires organizations and citizens to support, assist, and cooperate with the state intelligence work in accordance with the law and to keep confidential the national intelligence work known to them. Article 14 gives authority to state intelligence agencies to require citizens and organizations to support, assist, and cooperate in intelligence work. Article 16 authorizes government officials to "enter the relevant areas and places that restrict access," where they can examine and retrieve files, materials, and articles related to intelligence work, potentially including sensitive information. Finally, Article 17 allows Chinese intelligence agencies to assume control over an individual or organization's means of transport, communication tools, sites, and buildings and to set up workplaces and equipment in those facilities. In sum, Chinese entities providing goods in critical supply chains may be compelled to conduct intelligence work on behalf of the

[7] U.S. Dep't of Defense, National Security Agency, Cybersecurity Advisory: "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities" (Oct. 20, 2020), *https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF*.

PRC and provide sensitive information to PRC officials related to the security of U.S. critical infrastructure that rely on these sources.

In addition, the National Cybersecurity Law requires cybersecurity protection measures for critical information infrastructure and compels companies to report and provide assistance to the PRC state security and intelligence services. Article 31 identifies power and water resources, among other sectors, as critical information infrastructure. Article 38 requires critical information infrastructure operators to conduct an inspection and assessment of their networks' security and risks that might exist and submit a cybersecurity report on the circumstances. Additionally, Article 39 requires state cybersecurity and information departments to conduct spot testing of critical information infrastructure security risks and promote cybersecurity information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cybersecurity services organizations. Finally, Article 28 requires network operators to provide "technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." Thus, provisions within this law provide PRC officials access to information on cyber vulnerabilities across a number of sectors and thus the opportunity to obtain data potentially impacting the security of U.S. critical infrastructure companies.

AUTHORITY AND DETERMINATIONS:

1. Order of the Secretary.

Under authority delegated to the Secretary of the U.S. Department of Energy by the President in EO 13920, I adopt the findings in this Prohibition Order and order and direct the following:

2. Prohibited Transactions.

A Responsible Utility under this Prohibition Order is an electric utility that owns or operates Defense Critical Electric Infrastructure (DCEI), as defined by section 215A(a)(4) of the Federal Power Act (FPA), that actively serves a CDF, as designated by the Secretary under section 215A(c) of the FPA. Each Responsible Utility is hereby prohibited from acquiring, importing, transferring, or installing BPS electric equipment identified in Attachment 1 (Regulated Equipment) that (i) has been manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC, and (ii) is for use by the Responsible Utility as a component of its DCEI serving the CDF at a service voltage level of 69 kV or higher, from the point of electrical interconnection (at a service voltage level of 69 kV of higher) with the CDF up to and including the next "upstream" transmission substation. A transaction that meets the conditions set forth in the preceding sentence is referred to herein as a Prohibited Transaction.

The term Regulated Equipment includes software, firmware and digital components that control the operation of Regulated Equipment and are manufactured or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC.

3. Priority Loads, Load Shedding, and System Restoration Plans.

By this Prohibition Order, each Responsible Utility shall work with DOE to assist in the identification of DCEI and any load shedding and system restoration contingency planning required to assure the energy and missions of CDFs.

Each Responsible Utility is hereby directed to designate (or to take all action reasonably available to it to cause the relevant regional entity to designate) each CDF as a priority load in the applicable load shedding and system restoration plans. The term "regional entity" is defined at section 215(a)(7) of the FPA.

4. Effective Date.

The effective date of this Prohibition Order (Effective Date) is January 16, 2021. This Prohibition Order shall apply to any Prohibited Transaction initiated on or after the Effective Date. The Department shall notify each Responsible Utility of the applicability of this Prohibition Order no later than five (5) business days after the date of issuance of this Prohibition Order. Notice under this section shall be deemed made when personally delivered or when mailed, three (3) calendar days after deposit in the U.S. Mail, first class postage prepaid and addressed to the Responsible Utility at its applicable address. Actual notice shall be deemed adequate notice on the date actual notice occurred, regardless of the method of service.

5. Executive Order 13920.

On May 1, 2020, the President issued EO 13920. Actions authorized under EO 13920 are rooted in its finding that "unrestricted acquisition or use in the United States of bulk-power system electric equipment designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign

adversaries to create and exploit vulnerabilities in bulk-power system electric equipment," and that "the unrestricted foreign supply of bulk-power system electric equipment [therefore] constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." By declaring a "national emergency with respect to the threat to the United States bulk-power system" in the EO and under the National Emergencies Act, EO 13920 invokes the President's authority under the International Emergency Economic Powers Act (IEEPA) to direct responsive measures.

Section 1 of EO 13920 authorizes the Secretary of Energy (Secretary) to prohibit any transaction by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the equipment), where the transaction was initiated after May 1, 2020, and where the Secretary, in coordination with the Director of the Office of Management and Budget and in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, and, as appropriate, the heads of other relevant agencies, has determined that:

(a) The transaction involves BPS 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 BPS 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.

Section 2(a) of EO 13920 authorizes the Secretary "to take such actions, including directing the timing and manner of the cessation of pending and future transactions prohibited pursuant to section 1 of this order." Section 2(a) of EO 13920 also authorizes the Secretary to "adopt appropriate rules and regulations" to implement EO 13920, and DOE has initiated rulemaking proceedings. Notwithstanding the pendency of such a rulemaking or the adoption of any such regulations, the Secretary has the authority at any time to prohibit transactions in order to effectuate the purposes of EO 13920.

For the reasons noted above, the Secretary has determined that this Prohibition Order is reasonably necessary to address the threat posed to the BPS by the PRC as a foreign adversary within the meaning of EO 13920. Because the equipment identified in this Prohibition Order as Regulated Equipment could serve as instruments or tools to threaten the BPS and the national security of the U.S., the Secretary is taking the protective action set forth herein to prevent Prohibited Transactions.

This Prohibition Order is in addition to other action that the Secretary may undertake pursuant to EO 13920, including, but not limited to, rulemaking and further orders of the Secretary.

6. **BPS Electric Equipment Subject to This Prohibition Order.**

This order addresses a subset of EO 13920 BPS electric equipment (listed in Attachment 1) identified by the North American Electric Reliability Corporation (NERC) in its Recommendation to Industry.[8] The Regulated Equipment falls within the definition of "bulk-power system electric equipment" set forth in Section 4(b) of EO 13920:

> Items used in bulk-power system substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, current coupling capacitors, large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument transformers, coupling capacitor potential devices [expressed in the EO as current coupling capacitors and coupling capacity voltage transformers], protective relaying, metering equipment, high voltage circuit breakers, generation turbines, industrial control systems, distributed control systems, and safety instrumented systems. Items not included in the preceding list and that have broader application of use beyond the bulk-power system are outside the scope of [EO 13920].

Section 4(a) of EO 13920 defines "bulk-power system" as

> (i) Facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and

[8] NERC Alert ID R-2020-07-08-01 (July 8, 2020) (NERC Alert).

(ii) Electric energy from generation facilities needed to maintain transmission reliability. For purposes of [EO 13920], this definition includes transmission lines rated at 69,000 volts (69 kV) or more, but does not include facilities used in the local distribution of electric energy.

7. Certification by Responsible Utility.

Not later than March 17, 2021 and once every three years thereafter for as long as this Prohibition Order is in effect, each Responsible Utility shall file a certification with the Department, under penalty of perjury, that since the Effective Date:

(a) It has not entered into a Prohibited Transaction; and

(b) It has established an internal monitoring process to accurately track future compliance with this Prohibition Order.

Not later than February 15, 2021, each Responsible Utility shall file a certification with the Department, under penalty of perjury, that since the Effective Date:

(a) It has designated (or taken all action reasonably available to it to cause the relevant regional entity to designate) each CDF as a priority load in the applicable system load shedding and restoration plans.

Certifications may be delivered to: Charles Kosak, Deputy Assistant Secretary, Energy Resilience Division, U.S. Department of Energy, Office of Electricity, Mailstop OE-20, Room 8G-042, 1000 Independence Avenue, SW, Washington, DC 20585; (202) 586-2036; or *bulkpowersystemEO@hq.doe.gov*.

8. Individual Waiver.

The Secretary may waive any term of this Prohibition Order with respect to a Responsible Utility for good cause shown.

9. Penalties.

(a) *Penalties*.

(1) *Civil Penalty*. A civil penalty not to exceed the amount set forth in Section 206(b) of IEEPA may be imposed on any person who violates, attempts to violate, conspires to violate, or causes any knowing violation of this Order. IEEPA provides for a maximum civil penalty not to exceed the greater of $250,000 (subject to adjustment under the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended) or an amount that is twice the amount of the transaction that is the basis of the violation with respect to which the penalty is imposed.

Notice of the penalty, including a written explanation of the penalized conduct and the amount of the proposed penalty, and notifying the recipient of a right to make a written petition within thirty (30) calendar days as to why a penalty should not be imposed, shall be served on the party or parties that the Secretary has determined to be in violation hereunder.

The Secretary shall review any presentation and issue a final administrative decision within thirty (30) calendar days of receipt of the petition.

(2) *Criminal Penalty*. A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of a violation of this Order—and thereby a violation of IEEPA—shall, upon conviction thereof, be fined not more than $1,000,000, or if a natural person, may be imprisoned for not more than twenty (20) years, or both.

(b) *Adjustments to penalty amounts*.

(1) The civil penalties provided in IEEPA are subject to adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990 (Pub. L. 101-410, as amended, 28 U.S.C. 2461 note).

(2) The criminal penalties provided in IEEPA are subject to adjustment pursuant to 18 U.S.C. 3571.

(c) The penalties available under this section are without prejudice to other penalties, civil or criminal, available under law. Attention is directed to 18 U.S.C. 1001, which provides that whoever, in any matter within the jurisdiction of any department or agency in the U.S., knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious, or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious, or fraudulent statement or entry, shall be fined under title 18, U.S. Code, or imprisoned not more than five (5) years, or both.

10. <u>Rehearing</u>.

Any person aggrieved by this Prohibition Order may petition the Secretary for a rehearing no later than March 2, 2021. The application for rehearing shall set forth specifically the ground or grounds upon which such application is based. Upon such application, the Secretary shall have power to grant or deny rehearing or to abrogate or modify this Prohibition Order without further hearing. Unless the Secretary acts upon the application for rehearing within thirty (30) calendar days after it is filed, such application may be deemed to be denied. Until the record in a proceeding seeking rehearing of this Prohibition Order shall have been filed for judicial review in a court of competent jurisdiction, the Secretary may at any time, upon reasonable notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any findings or this Prohibition Order.

Signing Authority

This document of the Department of Energy was signed on December 17, 2020, by Dan Brouillette, Secretary of Energy. That document with the original signature and date is maintained by DOE. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned DOE Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Energy. This administrative process in no way alters the legal effect of this document upon publication in the *Federal Register*.

Dan Brouillette
Secretary of Energy

Attachment 1 – Regulated Equipment

1. Power transformers with low-side voltage rating of 69 thousand volts (kV) or higher and associated control and protection systems like load tap changer, cooling system, and Sudden Pressure relay
2. Generator step up (GSU) transformers with high-side voltage rating of 69 kV or higher and associated control and protection systems like load tap changer, cooling system, and Sudden Pressure relay
3. Circuit breakers operating at 69 kV or higher
4. Reactive power equipment (Reactors and Capacitors) 69 kV or higher
5. Associated software and firmware installed in any equipment or used in the operation of items listed in 1 through 4.