6450-01-P

DEPARTMENT OF ENERGY

[DOE-HQ-2020-0028]

Securing the United States Bulk-Power System

AGENCY: Office of Electricity, Department of Energy.

ACTION: Request for Information (RFI).

SUMMARY: Pursuant to Executive Order 13920 (EO 13920) issued May 1, 2020, titled "Securing the United States Bulk-Power System," the Department of Energy (DOE or the Department) is seeking information to understand the energy industry's current practices to identify and mitigate vulnerabilities in the supply chain for components of the bulk-power system (BPS).

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. If you anticipate difficulty in submitting comments within that period, contact the person listed in **FOR FURTHER INFORMATION CONTACT** as soon as possible.

ADDRESSES: Interested persons are encouraged to submit comments, identified by "Bulk-Power System EO RFI," by any of the following methods:

Federal eRulemaking Portal:

https://www.regulations.gov/docketBrowser?rpp=25&po=0&D=DOE-HQ-2020-0028. Follow the instructions for submitting comments.

Email: *bulkpowersystemEO@hq.doe.gov*. Include ''Bulk-Power System EO RFI'' in the subject line of the message.

Mail: Charles Kosak, Deputy Assistant Secretary, Transmission Permitting and Technical Assistance Division, Office of Electricity, Mailstop OE–20, Room 8G-024, Department of Energy, 1000 Independence Avenue, SW., Washington, DC 20585.

FOR FURTHER INFORMATION CONTACT: Mr. Charles Kosak, Deputy Assistant Secretary, Transmission Permitting and Technical Assistance Division, Office of Electricity, e-mail: *bulkpowersystemEO@hq.doe.gov* or phone: (202) 586-2036.

SUPPLEMENTARY INFORMATION:

Table of Contents

III. Submission of Comments

I. Introduction

A. Background

EO 13920 (85 FR 26595, May 4, 2020) declares that threats by foreign adversaries to the BPS constitute a national emergency. The BPS provides the electricity that supports the United States (U.S.) national defense, our vital emergency services, critical infrastructure, economy, and way of life. The Office of the Director of National Intelligence's (ODNI) National Counterintelligence and Security Center (NCSC) assesses that China and Russia (near-peer foreign adversaries) possess highly advanced cyber programs and that both nations pose a major threat to the U.S. government, including, but not limited to, military, diplomatic, commercial, and critical, infrastructures. The BPS is a target of these adversaries' asymmetric cyber and physical plans and operations. A successful attack on the BPS would present significant risks to the U.S. economy and public health and safety and would render the U.S. less capable of acting in defense of itself and its allies. The Department of Defense's *2018 National Defense Strategy* states that the homeland is no longer a sanctuary and that malicious cyber activity against personal, commercial, or government infrastructure is growing significantly. According to ODNI's *2019 Worldwide Threat Assessment of the U.S. Intelligence Community* (see *https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf*), near-peer foreign adversaries have the capability and integrated plans necessary to launch cyber-attacks causing localized, disruptive effects on critical infrastructure—such as the disruption of a natural gas pipeline and electric infrastructure for days to weeks—in the U.S. These near-peer foreign

adversaries continue to map U.S. critical infrastructure with the long-term goal of being able to cause substantial damage. According to the *2020-2022 National Counterintelligence Strategy* (see *https://www.dni.gov/index.php/ncsc-features/2741-the-national-counterintelligence-strategy-of-the-united-states-of-america-2020-2020*), these foreign adversaries are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure. They are also attempting to access our Nation's key supply chains at multiple points—from concept to design, manufacture, integration, deployment, and maintenance—by, among other things, inserting malware into important information technology networks and communications systems. As such, DOE is using NCSC's supply chain risk management (SCRM) framework to inform this RFI (see *https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats*). The NCSC leads and supports the U.S. Government's counterintelligence (CI) and security activities that are critical to protecting our Nation; provides CI outreach to U.S. private sector entities at risk of foreign intelligence penetrations; and issues public warnings regarding intelligence threats to the U.S. and establishes the de facto standard for Federal SCRM processes.

EO 13920 directs DOE, in consultation with the heads of several other agencies, to issue regulations implementing the authorities the President delegated to the Secretary of Energy. The rulemaking process will allow the opportunity for stakeholder comment and input on the substance of the rule. Consistent with the Department's commitment to public participation in the rulemaking process, the Department is soliciting views on safeguarding the supply chain

from threats and vulnerabilities. The Department is also soliciting views on its economic analysis.

B. Executive Order 13920 of May 1, 2020 (Securing the United States Bulk-Power System)

On May 1, 2020, the President issued Executive Order 13920, which has four main pillars:

1) Prohibit any acquisition, importation, transfer, or installation of BPS electric equipment by any person or with respect to any property to which a foreign adversary or an associated national thereof has any interest, that poses an undue risk to the BPS, the security or resiliency of U.S. critical infrastructure or the U.S. economy, or U.S. national security;
2) Authorize the Secretary to establish and publish criteria for recognizing particular equipment and vendors in the BPS electric equipment market as "pre-qualified" for future transactions and to apply these criteria to establish and publish a list of pre-qualified equipment and vendors;
3) Direct the Secretary, in consultation with heads of other agencies, to identify existing BPS electric equipment in which a foreign adversary or associated national thereof has an interest that poses an undue risk to the BPS, the security or resiliency of U.S. critical infrastructure or the U.S. economy, or U.S. national security and develop recommendations to identify, isolate, monitor, or replace this equipment as appropriate; and

4) Establish a Task Force on Federal Energy Infrastructure Procurement Policies Related to National Security, which will focus on the coordination of Federal Government procurement of energy infrastructure, the sharing of risk information and risk management practices, and the development of recommendations for implementation to the Federal Acquisition Regulatory Council (FAR Council).

EO 13920 defines BPS as (i) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (ii) electric energy from generation facilities needed to maintain transmission reliability. 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.

EO 13920 defines BPS electric equipment as items used in BPS substations, control rooms, or power generating stations, including reactors, capacitors, substation transformers, coupling capacitor potential devices [expressed in the EO as current coupling capacitors and coupling capacity voltage transformers], large generators, backup generators, substation voltage regulators, shunt capacitor equipment, automatic circuit reclosers, instrument 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 BPS are outside the scope of EO 13920.

"Foreign adversaries" are defined as any foreign government or foreign non-government person engaged in a long-term pattern or serious instance of conduct significantly adverse to the national security of the U.S. or its allies or the security and safety of U.S. persons. The current list of "foreign adversaries" consists of the governments of the following countries: 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). This determination is based on multiple sources, including ODNI's *2016-2019 Worldwide Threat Assessments of the U.S. Intelligence Community*, the *2020-2022 National Counterintelligence Strategy*, and the *2018 National Cyber Strategy of the United States of America* (see *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf*). Note, the abovementioned countries identified as "foreign adversaries" are here identified as such only for the purposes of EO 13920. The identification does not reflect a determination by the U.S. about the nature of other countries for any purposes other than this Executive Order. Additionally, the Secretary will periodically review this list in consultation with appropriate agency heads and may add to, subtract from, supplement, or otherwise amend the list at any time.

II. Request for Information

The Department seeks public input on the following questions regarding the first three pillars of EO 13920. Please carefully read Section III below regarding the public nature of submissions. As explained in detail below, any information that you do not want to be publicly viewable should not be included in your comment, nor in any document attached to your comment. Instructions regarding how to provide Confidential Business Information are also provided below. To the

extent possible, please reference the question being addressed in your response.

A. Supply Chain

Although this RFI covers the full scope of BPS electric equipment as defined in EO 13920, the Department seeks comments on specific equipment as outlined below to enable a phased process by which the Department can prioritize the review of BPS electric equipment by function and impact to the overall BPS. In doing so, the Department employs a defense-in-depth, phased approach that addresses risk as well as the dynamic nature of threats and vulnerabilities affecting the BPS. Accordingly, the Secretary may establish specific pre-qualification criteria for a set of components that support defense critical electric infrastructure (DCEI) and other critical loads and critical transmission feeders (69 kV and above) reported under critical infrastructure protection reliability standards as formulated by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission (FERC). Specific essential reliability services of interest may also include black start systems. The Department seeks comment on addressing the following types of equipment: transformers (including generation step-up transformers), reactive power equipment (reactors and capacitors), circuit breakers, and generation (including power generation that is provided to the BPS at the transmission level and back-up generation that supports substations). This includes both the hardware and electronics associated with equipment monitoring, intelligent control, and relay protection. Only transformers rated at 20 MVA and with a low-side voltage of 69 kV and above are included.

The Department does not plan to develop a SCRM tool or repeat questions already deemed best practices from well-established SCRM frameworks and tools, including the ODNI NCSC Supply

Chain Directorate's *SCRM Best Practices* (see *https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf*).

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*). The Department is focused on improving utility owner/operator's asset/operations risk assessment by incorporating the identification of enterprise risk associated with supply chain vendor/services into the acquisition systems process. For example, the Cybersecurity Capability Maturity Model (C2M2) is an available tool that an organization might apply to continuously assess its cybersecurity posture (see *https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0*).

The Department believes that it is prudent, and in the public interest, to address national security implications in acquisitions. This RFI is designed to specifically address: (1) evidence-based cybersecurity maturity metrics and (2) foreign ownership, control, and influence (FOCI). As part of the Federal acquisition process and NERC-CIP standards, the Department is considering:

- limited procurements,
- select build versus buy,
- the consequences of insufficient SCRM, and
- evidence-based performance metrics that support a continuous improvement process.

With that background, the Department seeks information responsive to the following questions:

A-1) Do energy sector asset owners and/or vendors conduct enterprise risk assessments, including a cyber maturity model evaluation on a periodic basis? Provide an explanation or description of an assessment program if it addresses the mitigation of risks associated with FOCI with respect to foreign adversaries (see *https://www.dcsa.mil/mc/ctp/foci/*).

A-2) Do energy sector asset owners and/or vendors identify, evaluate, and/or mitigate the following:

a. FOCI with respect to foreign adversaries with respect to access to company and utility data, product development, and source code (including research partnerships);

b. potential supply chain risks from sub-tier suppliers, recognizing that some sub-tier supply chain manufacturers could have FOCI with respect to foreign adversaries; and

c. assets and services critical risk tolerance regarding protecting these assets and services from FOCI?

A-3) Are non-standard incentives or changes to established standard development organizations' SCRM standards (including NIST 800 series, ISA/IEC 62443, NERC-CIP, and other Cyber Risk Maturity Model evaluations/practices) necessary to build capacity to protect source code, establish a secure software and firmware

development lifecycle, and maintain software integrity? How are benchmarks documented and tracked, including:

a. the ability to provide software, firmware, and hardware "bill of materials" (e.g. NTIA Software Component Transparency [see *https://www.ntia.doc.gov/SoftwareTransparency*] or equivalent industry norm) and track supply chain provenance and white-labeling;

b. authentication practices that prevent tampering, unauthorized production, and counterfeits; and

c. monitoring and tracking sub-tier supplier's adherence to security requirements as part of the SCRM?

A-4) What information is available concerning the following: BPS electric equipment cyber vulnerability testing standards, analyses of vulnerabilities, and information on compromises of BPS electric equipment over the last five years, including results of independent BPS electric equipment testing and penetration testing of enterprise systems for vulnerabilities (including methodology for discovery and remediation)?

a. What process does the energy sector have to share information with utilities regarding vulnerabilities and vice versa? Are contingency plans in place? How is the effectiveness of vulnerability testing and mitigation efforts monitored, tracked, and audited?

b. Is a record of an analysis of component vulnerabilities and any compromises of components and systems maintained for a specific period of time (e.g., five

years)? If yes, are the results of independent component testing and penetration testing of enterprise systems for vulnerabilities (including timeline for discovery and remediation) also maintained?

c. How are the results of independent component testing and penetration testing of enterprise systems for vulnerabilities (including timeline for discovery and remediation) maintained?

d. How are vulnerabilities identified by external entities addressed? How is the distribution of information regarding patching security vulnerabilities in the supply chain facilitated?

e. What insecure by design/vulnerable communication protocols exist today that should be retired or cannot be disabled or mitigated from BPS electric equipment (examples of protocols include Distributed Network Protocol 3 [DNP3], File Transfer Protocol [FTP], Telnet, or Modbus)?

A-5) What governance of sub-tier vendors do energy sector asset owners and/or vendors have in place? Is contract language for Supply Chain Security included in procurement contracts? Are metrics for supply chain security, along with cost, schedule, and performance maintained? What specific guidance should be developed for Integrator/Installer/Maintenance Service provider activities?

A-6) Can energy sector asset owners and/or vendors document the level of engagement in information sharing and testing programs that identify threats and vulnerabilities and incorporation of indicators of compromise (e.g., Information Sharing and Analysis Center, Information Sharing and Analysis Organization)? Does the energy

sector participate in a community for sharing supply chain risks? Does the energy sector encourage security related information exchange with external entities, including the Federal government?

A-7) What physical and logistical role-based access control policies have been developed to monitor and restrict access during installation when a foreign adversary, or associated foreign-owned, foreign-controlled, or foreign-influenced person is installing BPS electric equipment at a BPS site in the U.S.? What policies and practices exist to ensure installers/integrators effectively protect the systems and components during installation and commissioning? What policies and practices are in place to ensure that service providers (including those providing remote monitoring and management of systems) effectively maintain the security protections of the systems and components they are monitoring? Does an insider threat program exist?

A-8) Are there critical mineral or supply chain materials, and if so, what are they? Specify if any of these critical inputs rely on foreign sources, and the cause for that reliance, such as lack of domestic capability or quality factors. Per Executive Order 13817, the Department of Interior prepared *The Final List of Critical Materials 2018*, see: *https://www.federalregister.gov/documents/2018/05/18/2018-10667/final-list-of-critical-minerals-2018*.

B. Economic Analysis

As this RFI covers the full scope of BPS electric equipment as defined in EO 13920, the Department seeks information responsive to the following questions:

B-1) Within the EO 13920 definition of BPS electric equipment, what are the estimated one-time and recurring costs of developing, implementing, and periodically revising compliance plans and procedures associated with the Executive Order, including but not limited to:

a. Evaluating requirements.
b. Developing compliance plans and frameworks: supply chain documentation, foreign involvement evaluations, risk assessments, and process reviews.
c. Implementing plans: new supplier processes and contractual provisions; and supplier audits.
d. Supporting transaction reviews: records retention and responding to information inquiries.
e. Negotiating agreements to mitigate concerns raised in connection with transactions.
f. Other compliance costs.

B-2) Within the EO 13920 definition of BPS electric equipment, are there categories of BPS electric equipment that are more reliant on vendors likely to become the subject of transaction reviews, and if so, what are they? What are the sourcing challenges and cost impacts for companies facing prohibited transactions for those BPS electric equipment categories?

B-3) Does the energy sector have a procedure to identify services, components, and/or systems which are or should be covered by EO 13920? If yes, list the services,

components, and systems and provide the reasoning regarding why they should or should not be covered by EO 13920.

B-4) What unique challenges could EO 13920 present to small businesses?[1]

III. Submission of Comments

DOE invites all interested parties to submit in writing by [***INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER***], comments and information on matters addressed in this RFI.

Submitting comments via http://www.regulations.gov. The *http://www.regulations.gov* web page requires you to provide your name and contact information. Your contact information will be viewable to DOE only. Your contact information will not be publicly viewable except for your first and last names, organization name (if any), and submitter representative name (if any). If your comment is not processed properly because of technical difficulties, DOE will use this information to contact you. If DOE cannot read your comment due to technical difficulties and cannot contact you for clarification, DOE may not be able to consider your comment.

However, your contact information will be publicly viewable if you include it in the comment or in any documents attached to your comment. Any information that you do not want to be

[1] Using the North American Industry Classification System (NAICS) classifications, the Small Business Administration (SBA) defines small businesses in terms of firm revenues or employees. SBA's Table of Size Standards can be found at *https://www.sba.gov/document/support--table-size-standards*.

publicly viewable should not be included in your comment, nor in any document attached to your comment. Persons viewing comments will see only first and last names, organization names, correspondence containing comments, and any documents submitted with the comments.

Do not submit to *http://www.regulations.gov* information for which disclosure is restricted by statute, such as trade secrets and commercial or financial information (hereinafter referred to as Confidential Business Information ("CBI")). Comments submitted through *http://www.regulations.gov* cannot be claimed as CBI. Comments received through the website will waive any CBI claims for the information submitted. For information on submitting CBI, see the Confidential Business Information section.

DOE processes submissions made through *http://www.regulations.gov* before posting. Normally, comments will be posted within a few days of being submitted. However, if large volumes of comments are being processed simultaneously, your comment may not be viewable for up to several weeks. Please keep the comment tracking number that *http://www.regulations.gov* provides after you have successfully uploaded your comment.

Submitting comments via email or postal mail. Comments and documents submitted via email or postal mail also will be posted to *http://www.regulations.gov*. If you do not want your personal contact information to be publicly viewable, do not include it in your comment or any accompanying documents. Instead, provide your contact information on a cover letter. Include

your first and last names, email address, telephone number, and optional mailing address. The cover letter will not be publicly viewable as long as it does not include any comments.

Include contact information each time you submit comments, data, documents, and other information to DOE.

Comments, data, and other information submitted to DOE electronically should be provided in PDF (preferred), Microsoft Word or Excel, WordPerfect, or text (ASCII) file format. Provide documents that are not secured, written in English, and free of any defects or viruses. Documents should not contain special characters or any form of encryption and, if possible, they should carry the electronic signature of the author.

Campaign form letters. Please submit campaign form letters by the originating organization in batches of between 50 to 500 form letters per PDF or as one form letter with a list of supporters' names compiled into one or more PDFs. This reduces comment processing and posting time.

Confidential Business Information. According to 10 CFR 1004.11, any person submitting information that he or she believes to be confidential and exempt by law from public disclosure should submit via email two well-marked copies: one copy of the document marked confidential including all the information believed to be confidential, and one copy of the document marked "non-confidential" with the information believed to be confidential deleted. Submit these

documents via email. DOE will make its own determination about the confidential status of the information and treat it according to its determination.

It is DOE's policy that all comments may be included in the public docket, without change and as received, including any personal information provided in the comments (except information deemed to be exempt from public disclosure).

Signing Authority

This document of the Department of Energy was signed on July 2, 2020, by Bruce J. Walker, Assistant Secretary, Office of Electricity, pursuant to delegated authority from the 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*.

Signed in Washington, DC, on July 2, 2020.

Treena V. Garrett,
Federal Register Liaison Officer,
U.S. Department of Energy.

[FR Doc. 2020-14668 Filed: 7/7/2020 8:45 am; Publication Date: 7/8/2020]