e: 3510-33-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

[Docket No. 210910-0181]

RIN 0694-XC077

Notice of Request for Public Comments on Risks in the Information Communications Technology Supply Chain

AGENCY: Bureau of Industry and Security, Office of Technology Evaluation, U.S. Department of Commerce.

ACTIONS: Notice of request for public comments.

SUMMARY: On February 24, 2021, President Biden issued Executive Order 14017 (E.O. 14017) on "America's Supply Chains," which directs several federal agency actions to secure and strengthen America's supply chains. One of these directions is for the Secretary of Commerce and the Secretary of Homeland Security, in consultation with the heads of appropriate agencies, to submit, within one year of the date of E.O. 14017, a report on supply chains for critical sectors and subsectors of the information and communications technology (ICT) industrial base (as determined by the Secretary of Commerce and the Secretary of Homeland Security), including the industrial base for the development of ICT software, data, and associated services. This notice requests comments and information from the public to assist the Secretary of Commerce and the Secretary of Homeland Security in preparing the report required by E.O. 14017.

DATES: The due date for filing comments is [INSERT DATE OF FORTY-FIVE DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: *Submissions:* All written comments in response to this notice must be addressed to "Information and Communications Technology Supply Chain" and filed through the Federal eRulemaking Portal: *https://www.regulations.gov.* To submit comments via *https://www.regulations.gov,* enter docket number BIS–2021–0021 on the home page and click "search." The site will provide a search results page listing all documents associated with this docket. Find the reference to this notice and click on the link entitled "Comment Now!" (For further information on using *https://www.regulations.gov*, please consult the resources provided on the website by clicking on "How to Use This Site.")

FOR FURTHER INFORMATION CONTACT: Maura Weber, Defense Industrial Base Division, Office of Technology Evaluation, Bureau of Industry and Security, at 202-704-8388, Maura.Weber@bis.doc.gov, or ICTstudy@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

On February 24, 2021, President Biden issued Executive Order 14017, "America's Supply Chains" (86 FR 11849) (E.O. 14017). E.O. 14017 focuses on the need for resilient, diverse, and secure supply chains to ensure U.S. economic prosperity and national security. Such supply chains are needed to address conditions that can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. E.O. 14017 directs that within one year of the date of the order, the Secretary of Commerce and the Secretary of Homeland Security, in consultation with the heads of appropriate agencies, shall submit a report to the President, through the Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP), on supply chains for critical sectors and subsectors of the information and communications technology (ICT) industrial base (as

determined by the Secretary of Commerce and the Secretary of Homeland Security). For the purposes of this report, the scope of the ICT industrial base shall consist of hardware that enables terrestrial distribution, broadcast/wireless transport, satellite support, data storage to include data center and cloud technologies, and end user devices including home devices such as routers, antennae, and receivers, and mobile devices; "critical" software (as defined by the National Institute of Standards and Technology in relation to Executive Order 14028); and services that have direct dependencies on one or more of the enabling hardware. In developing this report, the Secretary of Commerce and the Secretary of Homeland Security will consult with the heads of appropriate agencies and will be advised by all relevant bureaus and components of the Department of Commerce and the Department of Homeland Security. This notice requests comments and information from the public to assist the Secretary of Commerce and the Secretary of Homeland Security in preparing the report required by E.O. 14017.

Written Comments

The Department of Commerce and the Department of Homeland Security are particularly interested in comments and information directed to the policy objectives listed in E.O. 14017 as they affect the U.S. ICT supply chains, as defined in the previous section, including, but not limited to, the following elements:

(i) "critical goods and materials," as defined in section 6(b) of E.O. 14017, underlying the supply chain in question. Under section 6(b) of E.O. 14017, "critical goods and materials" means goods and raw materials currently defined under statute or regulation as "critical" materials, technologies, or infrastructure;

(ii) "other essential goods and materials," as defined in section 6(d) of E.O. 14017, underlying the supply chain in question, including digital products. Under section 6(d) of E.O. 14017,

"other essential goods and materials" means those that are essential to national and economic security, emergency preparedness, or to advance the policy set forth in section 1 of E.O. 14017, but not included within the definition of "critical goods and materials";[1]

(iii) manufacturing, or other capabilities necessary to produce or supply the materials and services identified in paragraphs (i) and (ii) above, including emerging capabilities;

(iv) defense, intelligence, cyber, homeland security, health, climate, environmental, natural, market, economic, geopolitical, human-rights or forced-labor risks, or other contingencies that may disrupt, strain, compromise, or eliminate the supply chain—including risks posed by supply chains' reliance on digital products that may be vulnerable to failures or exploitation, and risks resulting from the elimination of, or failure to develop domestically the capabilities identified in paragraph (iii) above—and that are sufficiently likely to arise so as to require reasonable preparation for their occurrence;

(v) resilience and capacity of American manufacturing supply chains, including ICT design, manufacturing, and distribution, and the industrial base—whether civilian or defense—of the United States to support national and economic security, information security, emergency preparedness, and the policy identified in section 1 of E.O. 14017, in the event any of the contingencies identified in paragraph (iv) above occurs, including an assessment of:

(A) manufacturing or other needed capacities of the United States related to ICT design and manufacturing of products and services, including the ability to modernize to meet future needs;

[1] The Department of Commerce and the Department of Homeland Security are also interested in essential goods and materials essential to incident response and recovery.

(B) gaps in domestic design and manufacturing capabilities, including nonexistent, extinct, threatened, or single-point-of failure capabilities;

(C) information and cybersecurity practices and standards of the ICT sector with specific regard to the risks identified in paragraph (iv) above. The Department of Commerce and the Department of Homeland Security are specifically interested in comments related to validation standards of component and software integrity, standards and practices ensuring the availability and integrity of software delivery and maintenance, and security controls during the manufacturing phase of ICT hardware and components;

(D) supply chains with a single point of failure, single or dual suppliers, single region suppliers, highly connected markets or shared suppliers, or limited resilience, especially for subcontractors, as defined by section 44.101 of title 48, Code of Federal Regulations (Federal Acquisition Regulation);

(E) location of key design, manufacturing, software development, integration, and production assets, with any significant risks identified in paragraph (iv) above posed by the assets' physical location or the distribution of these facilities;

(F) exclusive or dominant supply of "critical goods and materials," and "other essential goods and materials," as identified in paragraphs (i) and (ii) above, by or through nations that are or are likely to become, unfriendly or unstable;

(G) availability of substitutes or alternative sources for "critical goods and materials," and "other essential goods and materials," as identified in paragraphs (i) and (ii) above.

(H) relevant workforce skills, best practices, and identified gaps in the availability and/or adequacy of domestic education and training resources necessary to fulfill future workforce needs;

(I) need for research and development capacity to sustain leadership in the development of services or "critical goods and materials," and "other essential goods and materials," as identified in paragraphs (i) and (ii) above;

(J) role of transportation and transmission systems in supporting existing supply chains and risks associated with those systems; and

(K) risks posed by climate change to the availability, production, transportation, or transmission of "critical goods and materials" and "other essential goods and materials," as identified in paragraphs (i) and (ii) above;

(vi) allied and partner actions, including whether or not the United States' allies and partners have also identified and prioritized the services or "critical goods materials" and "other essential goods and materials" identified in paragraphs (i) and (ii) above, and possible avenues for international engagement;

(vii) primary causes of risks for any aspect of the ICT industrial base and supply chains assessed as vulnerable pursuant to paragraph (v) above;

(viii) prioritization of the "critical goods and materials" and "other essential goods and materials," including digital products, identified in paragraphs (i) and (ii) above for the purpose of identifying options and policy recommendations. The prioritization shall be based on statutory or regulatory requirements; importance to national security, emergency preparedness, and the policy set forth in section 1 of E.O. 14017;

(ix) specific policy recommendations important for ensuring a resilient supply chain for the ICT industrial base. Such recommendations may include, but are not limited to, sustainably reshoring supply chains and developing or strengthening domestic design, components, and supplies; cooperating with allies and partners to identify alternative supply chains; building redundancy into domestic supply chains; ensuring and enlarging stockpiles; developing workforce capabilities; enhancing access to financing; expanding research and development to broaden

supply chains; addressing risks due to vulnerabilities in digital products relied on by supply chains; addressing risks posed by climate change; strengthening supply chain security; and any other recommendations;

(x) any executive, legislative, regulatory, and policy changes and any other actions to strengthen the capabilities identified in paragraph (iii) above, and to prevent, avoid, or prepare for any of the contingencies identified in paragraph (iv) above; and

(xi) suggestions for improving the Government-wide effort to strengthen supply chains, including suggestions for coordinating actions with ongoing efforts that could be considered duplicative of the work of E.O. 14017 or with existing Government mechanisms that could be used to implement E.O. 14017 in a more effective manner.

The Department of Commerce and the Department of Homeland Security encourage commenters, when addressing the elements above, to structure their comments using the specific text as identifiers for the areas of inquiry to which their comments respond. This will assist in more easily reviewing and summarizing the comments received in response to these specific comment areas. For example, a commenter submitting comments responsive to *paragraph (i) above*, would use that exact text – *The "critical goods and materials," as defined in section 6(b) of E.O. 14017, underlying the supply chain in question* – as a heading in the public comment followed by the commenter's specific comments in this area.

Requirements for Written Comments

The https://www.regulations.gov website allows users to provide comments by filling in a "Type Comment" field, or by attaching a document using an "Upload File" field. The Department of

Commerce prefers that comments be provided in an attached document. The Department of Commerce prefers submissions in Microsoft Word (.doc files) or Adobe Acrobat (.pdf files). If the submission is in an application format other than Microsoft Word or Adobe Acrobat, please indicate the name of the application in the "Type Comment" field. Please do not attach separate cover letters to electronic submissions; rather, include any information that might appear in a cover letter within the comments. Similarly, to the extent possible, please include any exhibits, annexes, or other attachments in the same file, so that the submission consists of one file instead of multiple files. Comments (both public comments and non-confidential versions of comments containing business confidential information) will be placed in the docket and open to public inspection. Comments may be viewed on https://www.regulations.gov by entering docket number BIS–2021–0021 in the search field on the home page.

All filers should name their files using the name of the person or entity submitting the comments. Anonymous comments are also accepted. Communications from agencies of the United States Government will not be made available for public inspection.

Anyone submitting business confidential information should clearly identify the business confidential portion at the time of submission, file a statement justifying nondisclosure and referring to the specific legal authority claimed, and provide a non-confidential version of the submission. The non-confidential version of the submission will be placed in the public file on https://www.regulations.gov. For comments submitted electronically containing business confidential information, the file name of the business confidential version should begin with the characters "BC". Any page containing business confidential information must be clearly marked "BUSINESS CONFIDENTIAL" on the top of that page. The non-confidential version must be clearly marked "PUBLIC". The file name of the non-confidential version should begin with the character "P". The "BC" and "P" should be followed by the name of the person or entity submitting the comments or rebuttal comments. If a public hearing is held in support of this

assessment, a separate *Federal Register* notice will be published providing the date and information about the hearing.

The Bureau of Industry and Security does not maintain a separate public inspection facility. Requesters should first view the Bureau's web page, which can be found at https://efoia.bis.doc.gov/ (see "Electronic FOIA" heading). If requesters cannot access the website, they may call 202-482-0795 for assistance. The records related to this assessment are made accessible in accordance with the regulations published in part 4 of title 15 of the Code of Federal Regulations (15 CFR 4.1 through 4.11).

Matthew S. Borman,

Deputy Assistant Secretary for Export Administration.

[FR Doc. 2021-20229 Filed: 9/17/2021 8:45 am; Publication Date: 9/20/2021]