



Billing Code: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 200609-0154]

RIN: 0660-XC046

Promoting the Sharing of Supply Chain Security Risk Information between Government and Communications Providers and Suppliers

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice, request for public comment.

SUMMARY: Section 8 of the Secure and Trusted Communications Network Act of 2019 (Act) directs the National Telecommunications and Information Administration (NTIA), in cooperation with other designated federal agencies, to establish a program to share supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services. Through this Notice and in accordance with the Act, NTIA is requesting comment on ways to facilitate the sharing of security risk information with such trusted providers. These comments will inform the program that NTIA establishes under the Act.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER THE DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**.

ADDRESSES: Written comments may be submitted by email to supplychaininfo@ntia.gov. Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW,

Room 4725, Attn: Evelyn L. Remaley, Associate Administrator, Office of Policy Analysis and Development, Washington, DC 20230. For more detailed instructions about submitting comments, see the “Instructions for Commenters” section at the end of this Notice.

FOR FURTHER INFORMATION CONTACT: Megan Doscher, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Washington, DC 20230; telephone (202) 482–2503; *mdoscher@ntia.gov*. Please direct media inquiries to NTIA’s Office of Public Affairs, (202) 482–7002, or at *press@ntia.gov*.

SUPPLEMENTARY INFORMATION:

Section 8 of the Secure and Trusted Communications Network Act of 2019 (Act) directs NTIA, in cooperation with the Office of the Director of National Intelligence, the Department of Homeland Security (DHS), the Federal Bureau of Investigation, and the Federal Communications Commission (FCC), to establish a program to share “supply chain security risk” information with trusted providers of “advanced communications service” and suppliers of communications equipment or services.¹ As part of that program, NTIA must “conduct regular briefings and other events” to share information with trusted providers and suppliers and “engage” with such providers and suppliers, particularly those that are small businesses or that primarily serve rural areas.² NTIA must also develop, and submit to Congress, a plan for declassifying material, when feasible, and expediting and expanding the provision of security clearances to facilitate information sharing from the Federal government to trusted providers and

¹ Secure and Trusted Communications Network Act of 2019, Pub. L. No. 116-124, § 8, 134 Stat. 158, 168 (2020) (*codified at* 47 U.S.C. 1607).

² *See id.* § 8(a)(2)(A), (B).

suppliers.³ Therefore, we request comments on several key terms in the Act, as well as on steps that should be taken to best achieve the purposes of the Act.

1. Key Terms:

NTIA seeks information to clarify key terms in the Act.

Supply Chain Security Risk Information

The Act defines “supply chain security risk” information to include “specific risk and vulnerability information related to equipment and software.”⁴ NTIA’s identification of supply chain security risk information will be aided by other ongoing U.S. Government activities to detect potential security risks to information and communications technology (ICT) supply chains. For example, this effort will be informed by all relevant activities of the National Strategy to Secure 5G, which focuses not only on the identification of information security risks, but on broader strategic risks to the U.S. economy and national security, including risks to the global 5G market, capabilities and infrastructure. Defining “supply chain security risk” to encompass national security and economic risk will reinforce the Act’s purpose to safeguard the economy and national critical infrastructure against these risks.⁵

NTIA will also be informed by key terms established by the Federal Acquisition Supply Chain Security Act of 2018, which established the Federal Acquisition Security Council (FASC), which is developing, within the Federal government, risk information sharing policies and

³ *See id.* § 8(a)(2)(C).

⁴ *Id.* § 8(c)(3).

⁵ *See* Executive Office of the President, *National Strategy to Secure 5G of the United States of America*, March 2020, available at <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf>.

procedures comparable to those that the Act contemplates for interactions between the Federal government and the private sector.⁶ That legislation defines “supply chain risk” by reference to 41 U.S.C. 4713, which in turn defines the term to mean “the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of covered articles or information stored or transmitted on the covered articles.”⁷

NTIA will also consider key terms defined by other bodies, such as the DHS ICT Supply Chain Risk Management Task Force (DHS Task Force), which provides a forum for government-private sector collaboration on supply chain issues and provides advice and recommendations on ways to assess and mitigate risks to the ICT supply chain.⁸ One of the DHS Task Force’s working groups is identifying and categorizing supply chain threats, as well as providing background information on such threats, their significance, and potential impact on the ICT supply chain.⁹

⁶ See Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, Tit. II, § 202, 132 Stat. 5173, 5180-81 (2018) (codified at 41 U.S.C. 1323(a)).

⁷ 41 U.S.C. 4713(k)(6).

⁸ See DHS, Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report*, at iii (Sept. 2019) (*DHS Task Force Interim Report*), available at https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf. For a list of Task Force members and contributors, see *id.* at v-vi.

⁹ See *id.* at 17-18.

Trusted Providers and Suppliers

- NTIA seeks comment on clarifying the term “trusted providers and suppliers.” The Act requires information sharing only with “trusted” providers and suppliers – entities “not owned by, controlled by, or subject to the influence of a foreign adversary.”¹⁰ In identifying the providers and suppliers that are ineligible under the Act, NTIA will rely on various designations as set forth in Section § 2(c)(1-4) of the Act. Accordingly, ineligible providers and suppliers will be determined by:

- (1) any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council;
- (2) the Department of Commerce pursuant to Executive Order No. 13873;
- (3) the equipment or service being covered is telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918); or
- (4) an appropriate national security agency.

Foreign Adversaries

NTIA directs commenters to the Act’s definition of “foreign adversary,” which is identical to that in Executive Order 13873, “Securing the Information and Communications Technology and Services Supply Chain” (EO 13873).¹¹ EO 13873 directs the Secretary of Commerce to review, and where necessary, prohibit transactions involving entities owned, controlled, or subject to foreign adversaries that pose unacceptable risks to the U.S. ICT and

¹⁰ Act, § 8(c)(4).

¹¹ Executive Order 13873, “Securing the Information and Communications Technology and Services Supply Chain,” 84 Fed. Reg. 22,689 (2019).

services supply chain.¹² NTIA notes that the determination of “foreign adversary” for purposes of implementing EO 13873 is a matter of executive branch discretion and will be made by the Secretary in consultation with the other agencies identified in the EO. To ensure consistency of action across the Federal government, in identifying the providers and suppliers that are eligible under the Act to receive supply chain security risk information, NTIA will rely on pertinent decisions by the Secretary of Commerce under EO 13873, as well as other relevant federal determinations.

Advanced Communications Service

Finally, NTIA seeks comment on the term, “advanced communications service.” The Act directs NTIA to share risk information only with trusted providers of “advanced communications service,” which the legislation equates with “advanced telecommunications capability” as defined in section 706 of the Telecommunications Act of 1996.¹³ As for mobile services, the FCC has determined that 4G Long Term Evolution services offering transmission speeds between 5Mbps/1Mbps and 10Mbps/3Mbps are the “best proxy” for advanced mobile service.¹⁴

Questions:

¹² Compare *id.* § 8(c)(2) with Executive Order 13873, § 3(b), 84 Fed Reg. 22,689, 22,691 (2019).

¹³ See Act, § 9(1). Advanced telecommunications capability “is defined, without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology.” Pub. L. No. 104-104, § 706(c)(1), 101 Stat. 56, 153 (1996) (*codified at* 47 U.S.C. 1302(d)(1)).

¹⁴ Inquiry Concerning Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Manner, 2019 Broadband Deployment Report, 34 FCC Rcd 3857, 3863-64, ¶ 16 (2019). Act, § 8(c)(4).

- What sorts of risks and vulnerabilities should be covered by the language “specific risk and vulnerability information related to equipment and software”?
- What information, if any, is unique to “supply chain risk information”? In other words, to avoid the re-creation of existing threat and vulnerability information sharing programs, what types of specific, enhanced, or aggregated threat and vulnerability information would be helpful to the private sector to identify, avoid, or mitigate ICT supply chain risks? What information do suppliers and providers need to make informed, risk-based security and transactional decisions?
- Are there supply chain security risks beyond those Congress specified that should be included in an information security program?
- To what extent should NTIA’s program be aligned with the actions of the FASC in determining whether an identified threat is a “security risk”?
- Section 4 of the Act sets a limit of 2,000,000 customers for the Act’s “remove and replace” reimbursement program. Is this also an appropriate measure to determine small business and rural service provider participation in the program, as required by Section § 8(a)(2)(B)?
Would that metric cause any key small or rural providers or suppliers to be missed?
- Are there other factors aligned with the Act that should be considered in determining “trusted” providers and suppliers eligible for the program?
- Should NTIA rely on the FCC’s benchmarks for “advanced” communications services to implement its information sharing program and, if so, what would be the implications for achieving the purposes of the Act?

2. Information Sharing Policies and Procedures:

As noted, the Act requires NTIA to share security risk information with trusted providers and suppliers via “regular briefings and other events.” It also requires NTIA to “engage” with trusted parties, particularly small businesses or those serving rural areas. Although the Act mentions small and rural providers and suppliers only in the context of engagements with the Federal government, NTIA believes those entities should be the principal focus of the information sharing program. The Act’s overarching goal is the establishment of an FCC program to reimburse smaller providers for removing from their networks and replacing equipment and services that threaten national security.¹⁵ Congress deemed reimbursement for such entities appropriate because it believed that smaller providers did not receive a sufficient “heads-up by our government” about the security risks posed by certain equipment and services and thus made procurement decisions based on the “bottom line.”¹⁶ The information sharing program mandated by Section 8 of the Act was intended to “fix this information gap by ensuring that [small, rural providers] have access to the information they need to keep their networks and Americans secure.”¹⁷ Accordingly, NTIA plans to structure that program primarily to promote the flow of risk information from the government to small and rural providers and suppliers. We request comment on that approach.

Because much security risk information is also highly sensitive, caution must be exercised in disseminating it. Briefings and events involving multiple participants or attendees, for example, risk exposing sensitive information or placing it in the wrong hands. NTIA seeks to balance the need to safeguard this information with the Act’s requirement to share it with trusted

¹⁶ See 165 Cong. Rec. H10286 (daily ed. Dec. 16, 2019) (remarks of Rep. Doyle).

¹⁷ *Id.* (remarks of Rep. Latta).

providers and suppliers. NTIA notes that security risk information is available either publicly or from non-government sources on various terms.¹⁸ For example, Congress and the Executive Branch raised concerns about the security risks posed by certain Chinese equipment suppliers as early as a decade ago.¹⁹

Questions:

- What means of sharing information best balances the objectives of the Act and the need to safeguard sensitive information? More specifically, what are the best ways for the Federal government to provide “regular briefings” to providers and suppliers? Would periodic public updates or notifications be useful or sufficient?
- Should eligible providers and suppliers have an opportunity to request risk and vulnerability information about specific equipment, software, and services? Would an information sharing system that incorporates both “push” and “pull” capabilities be useful, if possible?
- Are there legal barriers that could impede the ability of trusted providers and suppliers to receive or act on security risk information from the Federal government?
- How can publicly available security risk information be conveyed more expeditiously to more small and rural providers and suppliers?
- What barriers (*e.g.*, awareness, financial, legal) do small and rural providers and suppliers face in accessing security risk information from non-government sources? What could or should the Federal government do to eliminate or mitigate those barriers?

3. Information Declassification and Security Clearances:

¹⁸ See, *e.g.*, *DHS Task Force Interim Report* at 14-15.

¹⁹ See *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11425-26, ¶¶ 6-9 (2019).

NTIA's information sharing program must include a plan for declassifying materials, where feasible, and expanding and expediting the provision of security clearances to facilitate the dissemination of security risk information to trusted providers and suppliers. Because both actions potentially risk compromising the confidentiality of sensitive government information, NTIA is seeking additional information.

Questions:

- How specific must security risk information be to enable providers and suppliers to make procurement decisions that adequately protect their networks, customers, and users? If, for example, the Federal government issues a security warning about a particular company, how much information do trusted providers or suppliers require about the reason for that warning in order to take appropriate action?
- Is it more helpful for small and rural providers to receive unclassified information through typical civilian channels (for example, by e-mail) or to receive more detailed classified information that would require a staff member to obtain a security clearance and could require travel to receive the classified information in person at a secure location?
- What would be the best way of identifying appropriate staff points of contact at small and rural providers to ensure that they receive security risk information?
- Have small and rural providers and suppliers encountered problems in attempting to obtain security clearances for staff? If so, what has been the nature of those difficulties?
- How many performance-essential security clearances would an organization need to ensure that government-shared security risk information is fully incorporated into its corporate risk-based decision making and response? What challenges would an organization have, if any, in converting such information into action?

- How should NTIA best raise awareness of this program among small business and rural providers?

Instructions for Commenters: NTIA invites comment on the full range of issues that may be presented in this Notice, including issues that are not specifically raised in the above questions. Commenters are encouraged to address any or all of the above questions. Comments that contain references to studies, research, and other empirical data that are not widely available should include copies of the referenced materials with the submitted comments. Comments submitted by email should be machine-readable and should not be copy-protected. Responders should include the name of the person or organization filing the comment, which will facilitate agency follow up for clarifications as necessary, as well as a page number on each page of their submissions. All comments received are a part of the public record and will generally be posted on the NTIA website, <http://www.ntia.gov/>, without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information.

Dated: June 9, 2020.

Kathy Smith,

Chief Counsel,

National Telecommunications and Information Administration.

[FR Doc. 2020-12780 Filed: 6/11/2020 8:45 am; Publication Date: 6/12/2020]