**Before the**
**Federal Communications Commission**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs | ) | WC Docket No. 18-89 |
| | ) | |
| | ) | |

**DECLARATORY RULING AND**
**SECOND FURTHER NOTICE OF PROPOSED RULEMAKING**

**Adopted: July 16, 2020** **Released: July 17, 2020**

**Comment Date: [21 days after date of publication in the Federal Register]**
**Reply Comment Date: [35 days after date of publication in the Federal Register]**

By the Commission: Chairman Pai and Commissioners O'Rielly, Carr, Rosenworcel, and Starks issuing separate statements.

**TABLE OF CONTENTS**



## I. INTRODUCTION

1. America's communications networks have become the indispensable infrastructure of our economy and our everyday lives. The COVID-19 pandemic has demonstrated as never before the importance of these networks for employment and economic opportunity, education, health care, social and civic engagement, and staying connected with family and friends. It is therefore imperative that we safeguard this critical infrastructure from potential security threats.

2. The Commission has taken a number of targeted steps in this regard. For example, in November 2019, we prohibited the use of public funds from the Commission's Universal Service Fund (USF) to purchase or obtain any equipment or services produced or provided by companies posing a national security threat to the integrity of communications networks or the communications supply chain. We also initially designated Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of this rule, and we established a process for designating additional covered companies in the future. Additionally, last month, the Commission's Public Safety and

Homeland Security Bureau issued final designations of Huawei and ZTE as covered companies, thereby prohibiting the use of USF funds on equipment or services produced or provided by these two suppliers.

3. Today, we take further steps to protect the nation's communications networks from potential security threats as we integrate provisions of the recently enacted Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act) into our existing supply chain rulemaking proceeding. First, we adopt a Declaratory Ruling finding that, in the *2019 Supply Chain Order*, we fulfilled our obligation pursuant to section 3 of the Secure Networks Act to prohibit the use of funds made available through a Federal subsidy program administered by the Commission to purchase, rent, lease, or otherwise obtain or maintain any covered communications equipment or services from certain companies. Second, in the accompanying Second Further Notice of Proposed Rulemaking (Second Further Notice), we seek comment on proposals to implement further Congressional direction in the Secure Networks Act.

## II. BACKGROUND

4. Throughout the last decade, Congress and the Executive Branch have repeatedly stressed the importance of identifying and eliminating potential security vulnerabilities in communications networks and their supply chains.[1]

5. *Commission Action*. The Commission, which was created by Congress "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication . . . ,"[2] among other reasons, has taken a number of steps to address these concerns.

6. In April 2018, the Commission released the *2018 Supply Chain Notice*, which proposed and sought comment on a rule to prohibit the use of USF support to purchase or obtain equipment or services from any communications equipment or service provider identified as posing a national security risk to communications networks or the communications supply chain.[3] Consistent with that proposal, in November 2019, we adopted the *2019 Supply Chain Order*, which prohibits the use of "universal service support . . . to purchase or obtain any equipment or services produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain."[4] We adopted this rule based on our conclusion that it is critical to the provision of "quality service"[5] that USF funds be spent on secure networks and not be spent on equipment and services from companies that threaten national security. Pursuant to this rule, which is codified at 47 CFR § 54.9, USF funds may not be used to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by a covered company.

7. In the *2019 Supply Chain Order*, we also initially designated Huawei and ZTE, and their subsidiaries, parents, or affiliates, as companies that pose a national security threat to the integrity of communications networks and the communications supply chain, and we established a process for future designations of other companies posing such a risk.[6] Consistent with that process,[7] the Commission's

---

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11429-32, paras. 5–17 (2019) (*2019 Supply Chain Order*).

[2] 47 U.S.C. § 151.

[3] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 10-89, Notice of Proposed Rulemaking, 33 FCC Rcd 4058, 4058, para. 2 (2018) (*2018 Supply Chain Notice*).

[4] *2019 Supply Chain Order*, 34 FCC Rcd at 11433, para. 26.

[5] 47 U.S.C. § 254(b)(1).

[6] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11438-48, paras. 43–63.

Public Safety and Homeland Security Bureau (PSHSB) issued final designations of Huawei and ZTE on June 30, 2020.[8]

8. In the *2019 Supply Chain Further Notice*, which accompanied the *2019 Supply Chain Order*, we sought comment on a proposal to "require, as a condition on the receipt of any USF support that [eligible telecommunications carriers (ETCs)] not use or agree not to use within a designated period of time, communications equipment or services from covered companies."[9] We also proposed to establish a program to reimburse transition costs for ETCs required to remove and replace covered equipment and services.[10] To better inform our consideration of a reimbursement program, we required ETCs to report whether they use or own Huawei or ZTE equipment or services in their networks and to report the cost of removing and replacing such equipment and services.[11]

9. *Congressional and Executive Branch Action*. In 2017, responding to continuing concerns over the purchase and use of communications equipment from certain foreign entities, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA). The 2018 NDAA, among other things, 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.[12]

10. In 2018, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA).[13] Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from using federal funds to procure or obtain equipment, services, or systems 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.[14] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services" as (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) for certain safety and security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua) or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance equipment services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced

(Continued from previous page)

[7] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11438, para. 40; *id.* at 11449, para. 64; *id.* at 11486, para. 185 (directing PSHSB to determine whether to finalize the initial designations within 120 days of the *Order*'s publication in the Federal Register, and holding that the Bureau may extend the 120-day deadline for good cause); *Public Safety and Homeland Security Bureau Extends Timeframe For Determining Whether to Finalize Designations of Huawei and ZTE Pursuant to 47 C.F.R. § 54.9*, PS Docket Nos. 19-351 and 19-352, Public Notice, DA 20-471 (PSHSB May 1, 2020) (finding good cause to extend the timeframe for determining whether to finalize the initial designations of Huawei and ZTE to June 30, 2020).

[8] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, DA 20-690 (PSHSB Jun. 30, 2020) (*Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, DA 20-691 (PSHSB Jun. 30, 2020) (*ZTE Designation Order*).

[9] *2019 Supply Chain Order*, 34 FCC Rcd at 11470-71, para. 122.

[10] *Id*.

[11] *Id*. at 11481-82, paras. 162-63.

[12] *See* Pub. L. 115-91, 131 Stat. 1283, 1762, § 1656.

[13] *See* Pub. L. 115-232, 132 Stat. 1636.

[14] *Id*. at 1917, § 889(a)–(b)(1).

by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country, where "covered foreign country" is defined as the People's Republic of China.[15]

11. On March 12, 2020, the President signed into law the Secure Networks Act.[16] The Secure Networks Act mirrors key provisions of the *2019 Supply Chain Order and Further Notice*, and, among other measures, prohibits the use of USF funds to purchase covered communications equipment or services and directs the Commission to establish a reimbursement program similar to that proposed in the *2019 Supply Chain Further Notice*.

12. Several sections of the Secure Networks Act are relevant to today's Second Further Notice. Specifically, section 2 of the Secure Networks Act mandates that the Commission publish on its website a list of "covered" communications equipment. To be "covered," the Secure Networks Act provides that such equipment must meet two criteria. *First*, the communications equipment or service must, based exclusively on determinations made by Congress, certain government agencies, or interagency bodies, "pose[ ] an unacceptable risk to the national security of the United States or the security and safety of United States persons[.]"[17] *Second*, the equipment or services must be "capable of—(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[18]

13. Section 3 of the Secure Networks Act prohibits the use of funds made available through a Federal subsidy program administered by the Commission to purchase, rent, or otherwise obtain any covered communications equipment or services published on the list established pursuant to section 2.[19] Consistent with our proposals in the *2019 Supply Chain Further Notice*, section 4 establishes the Secure and Trusted Communications Networks Reimbursement Program to facilitate the removal, replacement, and disposal of covered communications equipment and services, complete with reporting and certification requirements.[20] Section 5 requires all providers of "advanced communications services" to submit annual reports to the Commission "regarding whether such provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service . . . ."[21] Section 7 tasks the Commission with enforcing the Secure Networks Act, and adds penalties beyond those in the Communications Act and our rules for violations of section 4.

14. After passage of the Secure Networks Act, PSHSB sought comment on the impact of the statute on the then-pending designation proceedings of Huawei and ZTE.[22] The Wireline Competition

---

[15] *See* Pub. L. 115-232, 132 Stat. 1636, 1918, Secs. 889(f)(2)-(3). The definition is also subject to certain exceptions, including that the equipment is only covered if it is capable of routing, redirecting, or permitting visibility into user data traffic or packets. *See id.* at 1917, Secs. 889(a)(2)(A)–(B).

[16] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609).

[17] Secure Networks Act § 2(b)(1).

[18] *See id.* § 2(a).

[19] *See id.* § 3(a)(1)(A)–(B).

[20] *See id.* § 4(a).

[21] *See id.* § 5(a).

[22] *See Public Safety and Homeland Security Bureau Seeks Comment on Applicability of Secure and Trusted Communications Networks Act of 2019 to Initial Designation Proceedings of Huawei and ZTE*, PS Docket Nos. 19-351, 19-352, Public Notice, DA 20-67 (PSHSB Mar. 13, 2020).

Bureau (WCB) also sought comment on the application of section 4 of the Secure Networks Act to the remove-and-replace reimbursement program proposed in the *2019 Supply Chain Further Notice*.[23]

15. Like Congress, the President and the Executive Branch have undertaken numerous efforts to secure the communications supply chain. For example, in December 2018, the Federal Acquisition Security Council, which includes seven Executive Branch agencies, was established pursuant to the SECURE Technology Act.[24] The Federal Acquisition Security Council is charged with developing a government-wide strategy to address communications supply chain risks and possesses the authority to recommend that other agencies remove insecure communications services or equipment.[25] In May 2019, the President signed Executive Order 13873, declaring a national emergency with respect to the security, integrity, and reliability of information and communications technology and services and granting the Secretary of Commerce the authority to prohibit transactions of information and communications technology or services when, among other things, the transaction would pose undue risks to U.S. critical infrastructure or national security.[26] In November 2019, the Department of Commerce began a rulemaking to implement Executive Order 13873.[27]

## III. DECLARATORY RULING

16. In the *2019 Supply Chain Order*, the Commission prohibited the use of universal service support for equipment and services produced or provided by companies designated as a national security threat.[28] We find that the Commission's prohibition, codified in section 54.9 of the Commission's rules, is consistent with and substantially implements subsection 3(a) of the Secure Networks Act, which prohibits the use of federal funds on certain communications equipment and services.[29] Accordingly, we further find that we have satisfied the requirements of section 3(b) in the Secure Networks Act and we need not revisit or otherwise modify our prior action in the *2019 Supply Chain Order*.[30]

17. Introduced prior to the adoption of the *2019 Supply Chain Order* and subsequently enacted on March 12, 2020, section 3(a) of the Secure Networks Act prohibits "[a] Federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service" from being used either to "purchase, rent, lease or otherwise obtain any covered communications equipment or service; or maintain any covered communications equipment or service . . . ."[31] The prohibition applies

---

[23] *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, WC Docket No. 18-89, Public Notice, DA 20-406 (WCB Apr. 13, 2020) (*Section 4 Public Notice*).

[24] *See* Pub. L. 115-390, 132 Stat. 5173.

[25] *See id.*

[26] *See* Executive Order 13873, 84 Fed. Reg. 11578, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (Executive Order 13873). On May 14, 2020, the President issued an order extending the emergency declaration for another year. *See* Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 29321 (May 14, 2020).

[27] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019).

[28] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11433, para. 26.

[29] 47 CFR § 54.9(a); Secure Networks Act § 3(b).

[30] 47 CFR § 54.9(a); Secure Networks Act § 3(b).

[31] Secure Networks Act § 3(a)(1).

"60 days after the date the Commission places such equipment or service on the list" required by section 2(a) of the statute.[32]

18. In section 3(b), Congress directed the Commission to adopt a Report and Order to implement this prohibition within 180 days following the Secure Networks Act's enactment.[33] Section 3(b) further states, "If the Commission has, before the date of the enactment of this Act, taken action that in whole or in part implements subsection (a), the Commission is not required to revisit such action, but only to the extent such action is consistent with this section."[34] We interpret the language in section 3(b) to mean that if the Commission has, prior to the enactment of the Secure Networks Act, already adopted a prohibition on the use of Federal funds that substantially tracks the statutory prohibition, then the Commission is deemed to have satisfied the 180-day deadline contained in section 3(b) and need not revisit its prior action.[35] To avail itself of this exception to the statutory deadline, however, the Commission's previously adopted prohibition must be "consistent" with, i.e., compatible with, and must not conflict with, the requirements of section 3(a).[36]

19. In the *2019 Supply Chain Order*, we prohibited the use of universal service support to "maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by a company posing a national security threat to the integrity of the communications networks or the communications supply chain."[37] We also initially designated two companies, Huawei and ZTE, as companies posing a national security threat.[38] PSHSB recently issued final designations of these entities, thereby prohibiting the use of USF funds to maintain, improve, modify, operate, manage, or otherwise support equipment or services produced or provided by Huawei and ZTE effective June 30, 2020.[39]

20. The Commission's prohibition in the *2019 Supply Chain Order* is consistent with and

[32] Secure Networks Act § 3(a)(2).

[33] *Id*. § 3(b). Congress separately required the Commission to publish the initial list of covered communications equipment or services within one year of enactment. *Id*. § 2(a).

[34] *Id*. § 3(b).

[35] Our interpretation is further bolstered by the timing of the legislation in Congress vis-à-vis the Commission's ongoing rulemaking proceeding. For example, the House Committee on Energy and Commerce held a markup on November 20, 2019, days before the Commission adopted the *2019 Supply Chain Order*, on a version of the bill in which section 3(b) specifically directed the Commission to "adopt a Report and Order in the matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (WC Docket No. 18-89) that implements subsection (a)." H.R. Rep. No. 116-352 (2019). A draft of the *2019 Supply Chain Order*, which closely matched the final adopted version, was published on the FCC's website for public review on October 29, 2019, three weeks before the FCC's November 22, 2019 vote adopting the *Order*. The Committee reported the November 20 version of the bill to the full House of Representatives. *Id*. By the time it was considered on the House floor, on December 16, the Commission had issued the *2019 Supply Chain Order* and the language of section 3(b) had been revised accordingly. 165 Cong. Rec. H10282-H10286 (Dec. 16, 2019).

[36] Secure Networks Act § 3(b); *see, e.g.*, *Environmental Defense Fund v. E.P.A.*, 82 F.3d 451, 457 (D.C. Cir. 1996) ("We believe the petitioners construe the phrase 'consistent with' too narrowly. . . . Thus, the statutory language does not require exact correspondence between the [state implementation] schedule and the [transportation improvement program's] implementation schedule but only congruity or compatibility between them.") (citations omitted).

[37] 47 CFR § 54.9(a).

[38] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11441-48, paras. 47–65.

[39] *See Huawei Designation Order* at paras. 10, 63; *ZTE Designation Order* at paras. 9, 29.

substantially implements the prohibition required by section 3(a) of the Secure Networks Act.[40] We start by noting that the Commission administers two ongoing programs that provide a "Federal subsidy": the USF, a Federal subsidy program that subsidizes the cost of obtaining communications equipment and/or services for carriers serving high-cost areas, schools and libraries, rural health care providers, and low-income households, and the Interstate Telecommunications Relay Service Fund, a Federal subsidy program that subsidizes the cost of relay services for individuals who are deaf, hard of hearing, deaf/blind, or have a speech impediment. Given that the USF, unlike the Interstate Telecommunications Relay Service Fund, "provides funds to be used for the capital expenditures necessary for the provision of advanced communications service," we believe Congress clearly intended the section 3 prohibition to apply to the USF.

21. We also find the scope of communications equipment and services covered by the Commission's prohibition encompasses the scope of the Secure Networks Act's section 3 prohibition. The Commission's prohibition broadly covers "any equipment or services produced by any company posing a national security threat."[41] In comparison, the prohibition in section 3 of the Secure Networks Act applies to "any covered communications equipment or service."[42] Covered communications equipment or service is limited to that which is capable of certain functions and capabilities or otherwise poses a security threat.[43] Although the Commission's prohibition goes further than the requirements of

[40] Huawei contends that the *2019 Supply Chain Order* "cannot fulfill any obligation imposed by the Secure Networks Act" because the FCC lacked authority to adopt it and the *Order* was otherwise arbitrary and capricious and violated the Administrative Procedure Act and Constitutional due process protections. *See* Written *Ex Parte* Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, at 1-2 (filed July 8, 2020) (Huawei *Ex Parte*). As the Commission has explained, the FCC was created in part to protect the national defense, and the *2019 Supply Chain Order* is consistent with that objective and a reasonable exercise of the Commission's authority under section 254 of the Communications Act to ensure "quality service" and protect the "public interest" by safeguarding the integrity of the telecommunications supply chain and communications networks. *See 2019 Supply Chain Order*, 34 FCC Rcd at 11433-36, paras. 28-34; *Huawei v. FCC*, No. 19-60896 (5th Cir.), Doc. 00515436647, pp. 33-48 (filed July 7, 2020). As the agency has previously explained, the *2019 Supply Chain Order* is likewise consistent with section 254(e) of the Communications Act, section 105 of CALEA, and the national security concerns of other federal agencies. *See 2019 Supply Chain Order*, 34 FCC Rcd at 11434-11438, paras. 31-38; *Huawei v. FCC*, No. 19-60896 (5th Cir.), Doc. 00515436647, pp. 33-48 (filed July 7, 2020). We do not believe that the Secure Networks Act curtails the Commission's authority to manage federal support for communications networks in a manner consistent with other requirements under the Communications Act. *See infra* n. 46; *Huawei Designation Order* at paras. 40-42. As to Huawei's Administrative Procedure Act and due process challenges to the *2019 Supply Chain Order*, the Commission explained in that *Order* that even assuming that a designation could result in a deprivation of a cognizable liberty or property interest—an argument we reject—the designation process provides suppliers with notice, information on the factual basis for the action, and a meaningful opportunity to be heard. *See 2019 Supply Chain Order*, 34 FCC Rcd at 11459-63, paras. 94-103; *Huawei v. FCC*, No. 19-60896 (5th Cir.), Doc. 00515436647, pp. 66-71 (filed July 7, 2020). Finally, this is not the appropriate forum to challenge the *2019 Supply Chain Order*, and we dismiss Huawei's arguments to the extent they constitute a collateral attack or untimely petition for reconsideration of that *Order*.

[41] 47 CFR § 54.9.

[42] Secure Networks Act § 3(a).

[43] *See id*. § 2(b)(2).

the Secure Networks Act, it does not conflict with the statutory requirements of section 3(a).[44] Accordingly, by complying with the Commission's broader prohibition, USF support recipients will be in compliance with the Secure Networks Act prohibition. Section 3(a) of the Secure Networks Act also specifies that the ban takes effect 60 days after the Commission places the equipment or service on the list required by section 2 of the statute.[45] We believe that rule 54.9 substantially implements this section 3 requirement by providing a notice period for interested parties (which, if opposed, we would expect to last at least 60 days) and stating that the ban takes effect only when initial designations of covered companies are finalized. However, to the extent there are differences between our rules and section 3 of the Secure Networks Act, we seek comment on additional changes to our rules.[46]

22. With our adoption of the prohibition in the *2019 Supply Chain Order*, we have substantially implemented the section 3 statutory mandate to adopt a prohibition on covered communications equipment or services. As such, we avail ourselves of the proviso, set forth in section 3(b), not to revisit our prior action implementing the mandate.[47] Nevertheless, in the accompanying Second Further Notice, we seek comment on additional changes to the Commission's rules pursuant to section 3 of the Secure Networks Act.

## IV. SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

23. Today's Declaratory Ruling finds that the *2019 Supply Chain Order* satisfies the Secure Networks Act's requirement that the Commission prohibit the use of funds for covered equipment and services. We now seek comment on sections 2, 3, 5, and 7 of the Secure Networks Act, including on how these provisions interact with our ongoing efforts to secure the communications supply chain.[48] As required by section 2, we propose several processes by which to publish a list of covered communications equipment and services. Consistent with sections 3, 5, and 7 of the Secure Networks Act, we propose to (1) ban the use of federal subsidies for any equipment or services on the new list of covered communications equipment and services; (2) require that all providers of advanced communications service report whether they use any covered communications equipment and services; and (3) establish regulations to prevent waste, fraud, and abuse in the proposed reimbursement program to remove, replace, and dispose of insecure equipment.

24. After we have adopted rules to further implement the Secure Networks Act, the Commission may prohibit the use of federal funds for potentially insecure communications equipment and services through two separate methods. First, pursuant to the *2019 Supply Chain Order* and section 254 of the Communications Act, no USF funds may be used to purchase or maintain any equipment or services produced or provided by a covered company. Second, pursuant to the Secure Networks Act, providers of advanced communications service will be prohibited from using federal subsidies, including

---

[44] Nothing in the Secure Networks Act restricts the Commission from using its other available statutory authority to prohibit the use of USF funds for a wider range of equipment or services than is required by section 3(a) of the Secure Networks Act. Similarly, the scope of prohibited conduct under section 54.9 of the Commission's rules encompasses the conduct prohibited by 3(a), such that the effect of a designation under the Commission's rules would satisfy the requirements of the statutory prohibition. Accordingly, we disagree with Huawei and find that section 54.9 of the Commission's rules is consistent with, i.e., is compatible and does not conflict with, section 3(a). *See* Huawei *Ex Parte* at 2-4. *See, e.g.*, *Environmental Defense Fund*, 82 F.3d at 457 (explaining that consistent with "means 'agreeing or according in substance or form,' that is 'congruous' or 'compatible'") (citations omitted); *Orthopaedic Hosp. v. Belshe*, 103 F.3d 1491, 1496 (9th Cir. 1997) ("'Consistent' means in agreement with, compatible, or conforming to the same principles or course of action.'") (citation omitted).

[45] Secure Networks Act § 3(a)(2).

[46] *See infra* paras. 47–51.

[47] Secure Networks Act § 3(b).

[48] WCB previously sought comment on the applicability of section 4 of the Secure Networks Act to its ongoing supply chain rulemaking proceeding. *See generally Section 4 Public Notice*.

the USF, to purchase or maintain communications equipment and services listed pursuant to section 2. We seek comment on this view.

25. As an initial matter, we seek comment on the definition of two terms used throughout the Secure Networks Act. Specifically, the Act's requirements apply to "communications equipment or service" and to providers of "advanced communications service." The Act defines "communications equipment or service" as "any equipment or service that is essential to the provision of advanced communications service."[49] The Act defines "advanced communications service" in turn as the "advanced telecommunications capability" described in section 706 of the Telecommunications Act of 1996, which encompasses "high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology."[50]

26. We propose to include within this definition of "communications equipment or service[s]" all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components. We believe that all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks. Moreover, the presence of electronic components provides a bright-line rule that will ease regulatory compliance and administrability. We seek comment on this interpretation.

27. We also propose to include within the definition of "advanced communications service" any connection at least 200 kbps in either direction. Such a reading is consistent with the Commission's historic interpretation of section 706 of the Telecommunications Act and the requirements that the Commission has imposed on providers of advanced telecommunications capability for purposes of reporting their broadband deployments.[51] We thus believe it consistent with congressional intent to capture the same pool of facilities-based providers who are currently required to report broadband deployment to comply with the requirements of the Secure Networks Act.[52]

28. We recognize the greater than 200 kbps reporting threshold reflects historical considerations as to speeds needed to provide advanced telecommunications capability.[53] The Commission has since determined, with advancements in technology, that fixed services with download speeds of at least 25 Megabits per second (Mbps) and upload speeds of at least 3 Mbps "meet the statutory definition of advanced telecommunications capability."[54] For mobile services, the Commission evaluates deployment using "multiple metrics instead of relying on a single benchmark," starting first "where service providers claim a minimum advertised speed of 5/1 Mbps."[55] However, importing a narrower definition of advanced communications service could leave insecure equipment in our nation's interconnected broadband networks even though it has been determined to pose a threat to national

[49] *Id.* § 9(4).

[50] *Id.* § 9(1).

[51] 47 CFR § 1.7001(b).

[52] 47 U.S.C. § 1302; 47 CFR § 1.7001.

[53] *See Inquiry Concerning Deployment of Advanced Telecommunications Capability to all Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996*, CC Docket No. 98-146, Report, 14 FCC Rcd 2398, 2406, para. 20 (1999) (stating, in relevant part, that "broadband" and "advanced telecommunications capability" "hav[e] the capability of supporting, in both the provider-to-consumer (downstream) and the consumer-to-provider (upstream) directions, a speed . . . in excess of 200 [kbps] in the last mile").

[54] *Inquiry Concerning Deployment of Advanced Telecommunications Capability to all Americans in a Reasonable and Timely Fashion*, GN Docket No. 19-285, 2020 Broadband Deployment Report, FCC 20-50, para. 15 (rel. Apr. 24, 2020).

[55] *Id*. at para. 16.

security. We seek comment on this interpretation and any alternatives.

### A. Section 2 of the Secure Networks Act

29. Section 2(a) of the Secure Networks Act directs the Commission to publish, no later than one year after enactment, a list of covered communications equipment and services (Covered List).[56] The remainder of section 2 lays out how the Commission is to construct this list. *First*, the Commission "shall place on the list any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on" a "determination" by other federal agencies or Congress, as outlined in section 2(c). *Second*, the Commission "shall place" on the Covered List "any communications equipment or service" "if, based exclusively on the determinations" under section 2(c), "such equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons"[57] and is "capable" of "(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[58] *Third*, section 2(d) requires that the Commission "shall periodically update the list published under subsection (a) to address changes in the determinations" under section 2(c). We seek comment on each part in turn.

#### 1. Section 2(c) of the Secure Networks Act

30. Section 2(c) of the Secure Networks Act states that "in taking action under subsection (b)(1), the Commission shall place" on the Covered List "any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations," and then lists four separate sources for such determinations.[59] We believe that the Secure Networks Act's use of the term "shall" provides the Commission no discretion to accept determinations from other sources not listed in the Secure Networks Act because the Commission must rely "solely" on one or more of the determinations listed in section 2(c) for the purposes of taking the steps required under section 2(b)(1) to compile the Covered List. We seek comment on this interpretation.

31. The external determinations as to whether communications equipment or services pose "an unacceptable risk to the national security of the United States and the security and safety of United States persons" come from the following agencies or legislation, pursuant to section 2(c):

> (1) "A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council";
> (2) "A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 . . . relating to securing the information and communications technology and services supply chain";
> (3) "The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3)" of the 2019 NDAA; or
> (4) "A specific determination made by an appropriate national security agency."

32. The Secure Networks Act defines "executive branch interagency body" as "an

[56] Secure Networks Act § 2(a).

[57] *Id.* § 2(b)(1).

[58] *Id.* § 2(b)(2)(A)–(C).

[59] *Id.* § 2(c).

interagency body established in the Executive Branch."[60] One of these bodies is the Federal Acquisition Security Council, established by 41 U.S.C. § 1322(a). The Federal Acquisition Security Council is tasked with developing criteria and processes for assessing threats and vulnerabilities to the supply chain posed by the acquisition of information technology.[61] We believe other executive agency bodies that could make determinations relevant to section 2(c) include the National Security Council, Homeland Security Council, Interagency Policy Committees, and other committees created for or chartered with a national security purpose. We seek comment on this view and ask if there are additional executive branch interagency bodies with appropriate national security expertise that can make the external determinations under section 2(c)(1). What role do the Committee on Foreign Investment in the United States (CFIUS) and Team Telecom have in this process? We also seek comment on the process and procedures we should use to incorporate executive branch interagency body determinations into the Covered List.

33. Section 2(c) also requires the Commission to rely on determinations made by the Department of Commerce. Executive Order No. 13873 grants the Secretary of Commerce the authority to prohibit any transaction of any information and communications technology or service where the Secretary, in consultation with other relevant agency heads, determines that the transaction: (i) involves property in which a foreign country or national has an interest; (ii) includes information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and (iii) poses certain undue risks to the critical infrastructure or the digital economy in the United States or certain unacceptable risks to U.S. national security or U.S. persons.[62] In November 2019, the Department of Commerce commenced a rulemaking to implement Executive Order No. 13873.[63] We seek comment on the process and procedures we should use to incorporate Department of Commerce external determinations into the Covered List.

34. We are also required to incorporate into the Covered List equipment or services identified in section 889(f)(3) of the 2019 NDAA. We seek comment on section 889(f)(3) generally and each of its subparts. Section 889(f)(3) of the 2019 NDAA defines "covered telecommunications equipment or services" to include "(A) telecommunications equipment produced by Huawei or ZTE; (B) for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua); [and] (C) telecommunications or video surveillance services provided by such entities or using such equipment."[64] Additionally, section 889(f)(3)(D) provides that covered telecommunications equipment or services includes "[t]elecommunications or video surveillance equipment or services produced or provided by an entity that the Department of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of [the People's Republic of

[60] *Id.* § 9(7).

[61] 41 U.S.C. § 1323(a).

[62] *See* Executive Order 13873, 84 Fed. Reg. 11578, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[63] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019).

[64] Pub. L. 115-232, 132 Stat. 1636, 1918, § 889(f)(3)(A)–(C).

China]."[65]

35. We seek comment on how the Commission must use section 889(f)(3) of the 2019 NDAA to add communications equipment and services to the Covered List. The plain language of section 2(c) provides that because telecommunications equipment from Huawei and ZTE are covered in section 889(f)(3)(A) of the 2019 NDAA, such equipment poses an unacceptable threat to U.S. national security or the safety and security of U.S. persons. We read section 2(c) as providing that video surveillance and telecommunications equipment from Hytera, Hikvision, and Dahua, to the extent it is used for public safety or security, poses an unacceptable threat to U.S. national security or the safety and security of U.S. persons. And we read section 2(c) as saying that "telecommunications or video surveillance services provided by" Huawei, ZTE, Hytera, Hikvision, or Dahua—those entities listed earlier in the paragraph—as well as any "telecommunications or video surveillance services" that use the equipment specified under subparagraphs (A) and (B) all pose an unacceptable threat to U.S. national security or the safety and security of U.S. persons. We seek comment on each of these interpretations. Does video surveillance equipment produced by Hytera, Hikvision, or Dahua or video surveillance service offered by Huawei, ZTE, Hytera, Hikvision, or Dahua qualify as "communications equipment or service" for the purposes of the Secure Networks Act? How should we interpret section 889(f)(3)(D) and any subsequent designations made by the Department of Defense? What other considerations are relevant to our interpretation of section 889(f)(3)?

36. The final potential source of an external determination in section 2(c) of the Secure Networks Act is an appropriate national security agency. Section 9(2) of the Secure Networks Act defines "appropriate national security agency" as the Department of Homeland Security, the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Federal Bureau of Investigation.[66] Some of these agencies, such as the Department of Homeland Security, include sub-agencies that may be involved in national security determinations, such as the Cybersecurity and Infrastructure Security Agency. We interpret the term "appropriate national security agency" to include any determination by a sub-agency of the Department of Homeland Security, the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Federal Bureau of Investigation, and seek comment on this interpretation. We also seek comment on the process and procedures we should use to incorporate their determinations into the Covered List.

37. We seek comment on what constitutes a specific determination that triggers the Commission's obligations under section 2(b)(1). Do the entities listed in section 2(c) have different processes to identify the equipment and services that we should publish as covered equipment? For example, the Federal Acquisition Security Council makes a confidential recommendation to the Secretary of Homeland Security, the Secretary of Defense, and the Director of National Intelligence, who then review the recommendation and decide whether or not to issue exclusion or removal orders.[67] Should we interpret the term "specific determination" broadly to ensure that any guidance or order from the entities listed in section 2(c) can be incorporated into our list? How specific must these determinations be? Must external determinations list specific information, such as model numbers of equipment, or detailed descriptions of prohibited services that the external source determines poses an unacceptable national security risk, or will the external source identify classes or categories of equipment at a less granular level? If an external source declines to specify equipment or services, or classes or categories thereof but instead simply provides the name of an entity, would that qualify as a "determination" under section 2(c)? Must a determination use the precise words of the statute (that certain "communications equipment or service . . . poses an unacceptable risk to the national security of the United States or the security and

[65] *Id.* § 889(f)(3)(D). We are unaware of any such determination as to entities beyond those named in section 889(f)(3) of the 2019 NDAA.

[66] Secure Networks Act § 9(2).

[67] 41 U.S.C. § 1323(c)(2), (4)–(5).

safety of United States persons") or should the Commission consider determinations that convey the same concept even if using different wording? Given the Commission's limited control over the format of a determination from an external source, what should the Commission do if it is unclear whether a particular decision by a section 2(c) source qualifies as a determination?

38. Relatedly, we seek comment generally on the mechanics of using these determinations to publish the Covered List. We expect that any determinations covered under sections 2(c) will be publicly released by the original decisionmaker. If such a determination is public, we do not believe the Commission must issue any notice regarding our receipt of this determination. We seek comment on this understanding. Section 2(a) provides that the first Covered List must be published on the Commission's website no later than March 12, 2021.[68] In order to meet this deadline, by what date do we need to receive the external determinations? Should we affirmatively solicit these determinations from other agencies and, if so, how? Are there any other procedures we should consider to comply with section 2(c) of the Secure Networks Act?

### 2. Section 2(b) of the Secure Networks Act

39. Section 2(b) of the Secure Networks Act states that the Commission "shall place" on the Covered List "any communications equipment or service" that (1) "is produced or provided by any entity" "if, based exclusively on the determinations" under section 2(c), "such equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons"[69] and (2) is "capable" of "(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[70]

40. We start with an observation: Specifically, if certain equipment or services have been found under section 2(c) to "pose[] an unacceptable risk to the national security of the United States and the security and safety of United States persons" (and thus fulfills the section 2(b)(1) criterion), isn't such equipment or service necessarily "capable" of "posing an unacceptable risk to the national security of the United States or the security and safety of United States persons" (and thus fulfilling the section 2(b)(2) criterion)?

41. We resolve this potential for surplusage by recognizing that external determinations may be done at different levels of generality. For example, a section 2(c) source may determine a particular model of equipment (or a particular service) "poses an unacceptable risk" at a very granular level. In making such a determination, we would expect the section 2(c) source to consider whether the particular model of equipment (or particular service) is "capable" of "(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons" precisely because those are the types of consideration necessary to determine whether that particular equipment or service actually "poses an unacceptable risk" under the law. And so, in such a case, we believe that the specific equipment or service must be placed on the Covered List because another agency has already concluded that the particular equipment or service poses an unacceptable national security risk (and thus it must be "capable" of posing such a risk under section 2(b)(2)(C) regardless of whether it also meets the section 2(b)(2)(A) or (B) criteria).[71]

[68] Secure Networks Act § 2(a).

[69] *Id.* § 2(b)(1).

[70] *Id.* § 2(b)(2)(A)–(C).

[71] *Id.* § 2(b)(2)(C).

Thus, the Commission's placement of the equipment or service on the Covered List in such a case is a non-discretionary, ministerial act. We seek comment on this view.

42. In contrast, a section 2(c) source may determine that a broader class of equipment or services "poses an unacceptable risk"—as section 889(f)(3)(A) of the 2019 NDAA does when it lists all "telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities)."[72] When an external source identifies classes or categories of equipment or services as part of its external determination, we believe that the best reading of the Secure Networks Act is to apply the external determination to particular models of equipment or services in light of the section 2(b)(2) criteria. So in applying the general determination that telecommunications equipment from ZTE or Huawei poses an unacceptable risk to a particular piece of equipment, the Commission would look to whether that equipment is "capable" of "(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[73] As such, the Covered List would include "Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation that is capable of (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles, (B) causing the networks of a provider or advanced communications service to be disrupted remotely, or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons." We seek comment on this proposal. In turn, we seek comment on how we should define "capable" for purposes of section 2(b)(2) of the Secure Networks Act.[74] We believe "capable" should be read broadly, and equipment or services may be "capable" of fulfilling section 2(b)(2)(A) or (B) even if they are not ordinarily used to perform the functions in 2(b)(2)(A) or (B), so long as they can possibly perform those functions. We seek comment on this view. How will interested parties determine whether specific equipment or services are capable of posing an unacceptable national security risk, pursuant to section 2(b)(2)(C)?[75]

43. We seek comment on alternatives to our lead proposal. For example, once we receive an external determination that communications equipment or services pose an unacceptable security risk, should we conduct an independent analysis of the capabilities of each specific piece of communications equipment or services before including it on the Covered List? If so, could we permissibly find that equipment is not "capable" of posing an unacceptable risk even if we must "exclusively" rely on a section 2(c) source to determine that it does actually pose such a risk? Must we identify the specific capability from section 2(b)(2)(A)-(C) that warrants inclusion on the Covered List for every piece of communications equipment and service? Is such an analysis of each and every piece of equipment included in a section 2(c) determination even possible in light of the one-year deadline for creating such a list? Even if such an analysis could be done, would a particularized Covered List be easily evaded given how frequently communications equipment is updated? Are there best practices for producing a detailed list that is informative and easy to consult and understand? What would be the administrative burden of an equipment-by-equipment determination under section 2(b)(2), and do any benefits of such an approach outweigh the burdens of the slower process of identifying covered equipment and services? We seek comment on other potential methods of interpreting and complying with section 2 of the Secure Networks Act and their costs and benefits.

44. Finally, regardless of how we interpret the interplay of section 2(b)'s various provisions,

[72] 2019 NDAA § 889(f)(3)(A).

[73] *See* Secure Networks Act § 2(b)(2).

[74] *Id.* § 2(b)(2).

[75] *Id.* § 2(b)(2)(C).

we seek comment on the process for allowing interested parties to clarify whether a specific piece of communications equipment or a specific service is on the Covered List. What is the best method for allowing the interested party to seek clarity? For example, the Commission's rules provide for declaratory rulings to remove uncertainty.[76] How can we provide interested parties adequate opportunity to demonstrate that specific equipment or services are or are not included on the Covered List while meeting our obligations under the Secure Networks Act?

### 3. Section 2(d) of the Secure Networks Act

45. Section 2(d) of the Secure Networks Act sets out certain requirements for the Commission to maintain the Covered List. Section 2(d)(1) requires the Commission to update the Covered List "periodically" to address changes in the determinations made by other governmental agencies.[77] The Commission must monitor the Covered List to add additional communications equipment or services or remove equipment or services if the basis for its inclusion no longer exists.[78] For each 12-month period during which the Covered List is not updated, the Commission must notify the public that no updates were necessary to protect national security or to address changes in existing determinations.[79] We read the language of section 2(d) to be mandatory—precluding us from altering the list beyond the specific updates (all tied to changes in section 2(c) determinations) required by its terms. We seek comment on this interpretation. We also seek comment on the process to update and publish the Covered List and solicit ideas and best practices for ways to maintain the Covered List and keep it current and readily available.

46. Consistent with the Secure Networks Act, which establishes no notice period before the publication of the Covered List, we propose to publish the Covered List without first seeking public comment on the contents. We note that section 2(d) uses mandatory language and thus does not appear to give the Commission discretion not to update the Covered List based on changes in determinations, and hence it would be unclear what purpose a notice period would serve. We seek comment on this proposal.

## B. Section 3 of the Secure Networks Act

47. In the Declaratory Ruling, we found that the prohibition adopted in section 54.9 of the Commission's rules substantially implements the prohibition contained in section 3 of the Secure Networks Act. That is, the Commission's current section 54.9 prohibition on spending USF funds, adopted pursuant to the Communications Act, broadly applies to all equipment and services produced or provided by entities designated as "posing a national security threat."[80] Section 3 of the Secure Networks Act, in comparison, applies to Federal programs subsidizing capital expenditures necessary for the provision of advanced communications service and more narrowly to covered communications equipment and services identified in the Covered List.[81]

48. We propose and seek comment on the designation of covered communications equipment and services on the Covered List. If our proposal here is adopted, the Commission would have two different designation processes, one for the designation of an entity, as currently provided by the Commission's rules and another, more targeted process, for the designation of specific communications equipment and services per section 2 of the Secure Networks Act. To accommodate this outcome, we propose a new rule, independent of the section 54.9 prohibition, that would prohibit, going forward, the use of federal subsidies made available through a program administered by the Commission to purchase,

[76] *See* 47 CFR § 1.2(a).

[77] Secure Networks Act § 2(d)(1).

[78] *Id.* § 2(d)(2).

[79] *Id.* § 2(d)(3).

[80] 47 CFR § 54.9.

[81] Secure Networks Act §§ 2(a), 3(a), 9(5).

rent, lease, otherwise obtain, or maintain any covered communications equipment and services identified and published on the Covered List. We propose that the new prohibition on the use of USF funds pursuant to the Secure Networks Act would be effective 60 days after communications equipment or services are placed on the Covered List.[82] We seek comment on this proposal, which tracks the text of section 3 of the Secure Networks Act and would more closely align the Commission's rules with the Secure Networks Act than currently provided for under section 54.9.[83]

49. As discussed in the Declaratory Ruling, we read the prohibition in section 3 as intending to apply to all universal service programs but not other Federal subsidy programs to the extent those programs may at times tangentially or indirectly involve expenditures related to the provision of advanced communications services.[84] We seek comment on this proposal. We believe that applying this prohibition to USF programs furthers our responsibility to ensure that public funds are not spent on equipment or services from companies that present a risk to the supply chain, whether that responsibility arises from our own statutory imperatives or from the Secure Networks Act. The prohibition would also apply to any other programs administered by the Commission that primarily support the provision of advanced communications services, as well as any future USF programs implemented by the Commission. We seek comment on this approach.

50. We seek comment on how the proposed rule would affect multiyear contracts or contracts with voluntary extensions between fund recipients and companies producing or providing communications equipment or services posing a supply chain security risk, if any such contracts exist. We specifically seek comment on whether the Secure Networks Act, which states that the prohibition shall apply 60 days after the date on which the Commission places a service or piece of equipment on the Covered List, permits us to grandfather any such arrangements. If we do grandfather contracts, should we only grandfather unexpired annual or multiyear contracts, or also grandfather one-year contracts with voluntary extensions? We note that in the *2019 Supply Chain Order*, the Commission declined to grandfather existing contracts, finding that "[e]xempting existing multiyear contracts would negate the purpose behind our rule and allow federal funds to be used to perpetuate existing security risks to communications networks and the communications supply chain."[85] To what extent would our adoption of the proposed rule trigger any change-of-law provisions?

51. Are there other practical issues raised by our proposals that the Commission should address in implementing this proposed rule? Would section 3, any other section of the Secure Networks Act,[86] or the Secure Networks Act as a whole provide us independent authority to require ETCs or other

[82] To be clear, certain equipment or services could be subject to both the prohibition in 47 CFR § 54.9 and section 3 of the Secure Networks Act, and parties subject to these requirements would be responsible for complying with both prohibitions (including whichever is effective first).

[83] *See* 47 CFR § 54.9. *See also* Letter from Douglas Kinkoph, Associate Administrator, Office of Telecommunications and Information Applications, National Telecommunications and Information Administration, to Ajit Pai, Chairman, Federal Communications Commission, PS Docket Nos. 19-351, 19-352; WC Docket No. 18-89, at 4, n. 19 (Jun. 9, 2020).

[84] For example, the Interstate Telecommunications Relay Services (TRS) Fund is a Federal subsidy program administered by the Commission. *See Contributions to the Telecommunications Relay Services Fund*, Report and Order, 26 FCC Rcd 14532 (2011). The Interstate TRS Fund, however, does not subsidize capital expenditures necessary for the provision of advanced communications services.

[85] *2019 Supply Chain Order*, 34 FCC Rcd at 11457, para. 87.

[86] *See, e.g.*, Secure Networks Act § 4(d)(4)(B)(i) (providing that as of the date a reimbursement program application is approved, the applicant for reimbursement "will not purchase, rent, lease, or otherwise obtain covered communications equipment or services, using reimbursement funds or any other funds (including funds derived from private sources).").

providers to remove and replace equipment on the Covered List?[87]

### C. Section 5 of the Secure Networks Act

52. Section 5 of the Secure Networks Act requires each "provider of advanced communications service" to report annually, "in a form to be determined by the Commission," if it has "purchased, rented, leased, or otherwise obtained any covered communications equipment or service."[88] All covered communications equipment or services on the initial Covered List published under section 2(a) of the Secure Networks Act that was purchased, leased, or otherwise obtained by a provider on or after August 14, 2018 must be reported, and any additional covered equipment or services must be reported within 60 days after the list is updated.[89]

53. The Secure Networks Act also requires providers to include "a detailed justification" for procuring such communications equipment or services, information about whether the equipment or service has subsequently been removed and replaced, and information about any plans for the continued purchase, rent, lease, installation, or use of such covered communications equipment or services.[90] If a provider does not have any covered communications equipment or services in its network, then subsequent annual reports beyond an initial certification are not required unless subsequent purchases or other actions make the initial certification inaccurate.[91]

54. While we recently conducted an information collection to better understand the extent of Huawei and ZTE equipment in our communications networks, we recognize the annual reporting requirement contained in section 5 goes beyond the scope and frequency of that collection.[92] We limited the earlier collection requirement to ETCs, their subsidiaries, and their affiliates, but allowed service providers with pending ETC designations and others to participate on a voluntary basis. The type of information reported in the earlier collection did not track the requirements of section 5. For example, the earlier collection did not require any justification as to purchasing decisions.[93] Accordingly, the collection would not satisfy section 5 of the Secure Networks Act absent significant modification.

55. We therefore propose and seek comment on a new information collection requirement to implement section 5. Specifically, we propose to require that all "providers of advanced communications services" must comply with the new reporting requirement contained in section 5 of the Secure Networks Act. The information contained in the report would generally encompass the requirements in section 5. Consistent with section 5, we propose to require that filers report the type, location, date obtained, and any removal and replacement plans of covered equipment and services in their network. Filers will also have to provide a "detailed justification" explaining why they obtained covered equipment or services. We seek comment on what the detailed justification should include and on these other proposals. Is there additional information the Commission should require, to be consistent with the Secure Networks Act's purpose and obligations, that would prove helpful in monitoring and assessing the presence and replacement of covered equipment and services? For example, would it be helpful to know the amount

---

[87] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11470-73, paras. 122-23, 128-31 (proposing to rely on sections 254 and 201(b) of the Communications Act to require ETCs to remove and replace covered equipment and services).

[88] Secure Networks Act § 5(a).

[89] *Id*.

[90] *Id*. § 5(c).

[91] *Id*. § 5(b).

[92] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11481-82, paras. 162–66; *Protecting Against National Security Threats to the Communications Supply Chain through FCC Programs*, WC Docket No. 18-89, Order, DA 20-370 (extending the reporting deadline to May 22, 2020).

[93] *See* FCC, Identifying Potentially Prohibited Communications Supply Chain Equipment and Services, www.fcc.gov/supplychain.

paid for the covered equipment and services or the supplier from whom the equipment was purchased? We also seek comment on how the Commission could use the information it has already collected to reduce potentially duplicative reporting requirements for carriers.[94]

56. To what extent should we make reported information publicly available or treat it as presumptively confidential and not subject to routine public inspection? Consistent with the *2019 Supply Chain Order*, we do not propose to treat as confidential whether a particular provider has covered equipment or services in its network.[95] Moreover, because information on the magnitude of covered equipment and services among individual service providers would be of public interest, we propose to make such information publicly available. Provider-specific information on the location of covered equipment and services could raise security and confidentiality concerns. Accordingly, we propose to treat that specific information as presumptively confidential.[96] We seek comment on these proposals and any alternative proposals.

### D. Section 7 of the Secure Networks Act

57. Section 7(a) requires the Commission to treat violations of the Secure Networks Act and violations of the regulations pursuant to that statute as violations of the Communications Act.[97] Accordingly, the Commission would have authority to subject those found in violation of the Secure Networks Act to forfeitures as authorized under section 503(b) of the Communications Act and section 1.80 of the Commission's rules.[98] Additional regulations to implement this particular provision appear unnecessary as there are already regulations governing Commission processes regarding forfeiture proceedings. We seek comment on the assumption that the Commission need not propose any new procedural enforcement requirements associated with section 7(a) of the Secure Networks Act.

58. Separately, section 7(b) requires the repayment of funds disbursed per the reimbursement program prescribed in section 4 of the Secure Networks Act by recipients if they are found to have violated section 4, the Commission's regulations promulgated pursuant to section 4, or the "commitments made by the recipient in the application for the reimbursement."[99] Section 4 establishes the reimbursement program providers may use to help pay for the removal, replacement, and disposal of covered communications equipment and services. The statute further calls for the referral of such violations to "all appropriate law enforcement agencies or officials for further action under applicable criminal and civil laws."[100] The statute bars violators from further participation in the section 4 reimbursement program, and violators may be barred from participating in other Commission programs,

---

[94] USTelecom asserts that the information collection conducted pursuant to the *2019 Supply Chain Order* is "supersede[d]" by the section 5 requirement. *See* Letter from Mike Saperstein, Vice President, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket 18-89, at 1 (filed July 9, 2020) (USTelecom *Ex Parte*). We disagree. For one, nothing in the text of the law even suggests as much. For another, the information collections cover different topics over different time periods—so the argument for implicit repeal rings hollow. For yet another, USTelecom offers no coherent reason why Congress in section 5 would intend to *sub silentio* discard information we have already collected, especially not when the Commission has been working to provide Congress information from that collection so as to better estimate the total costs of the Secure and Trusted Communications Networks Reimbursement Program, as required by section 4 of that very same statute. USTelecom *Ex Parte* at 1; *see* Secure Networks Act §§ 4-5.

[95] *See 2019 Supply Chain Order*, 34 FCC Rcd at 11482, para. 166.

[96] *See* OMB Control No. 3060-1270, ICR Ref. No. 201912-3060-014, Supporting Statement, at 4-5 (filed Feb. 12, 2020), https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=201912-3060-014.

[97] Secure Networks Act § 7(a).

[98] 47 U.S.C. § 503(b); 47 CFR § 1.80.

[99] Secure Networks Act § 7(b)(1).

[100] *Id*. § 7(b)(1)(C).

"including the Federal universal service support programs."[101] Before requiring repayment and triggering the additional penalty actions, the Commission must first give alleged violators notice and a 180-day opportunity to cure the violation.[102] We propose to adopt regulations tracking the language contained in section 7 and seek comment on this proposal.

59. The Commission is also required by section 7(c) to "immediately take action to recover all reimbursement funds awarded" when a recipient is required to repay reimbursement under section 7(b)(1)(A) due to a violation.[103] We propose to initiate such action by sending a request for repayment to the recipient immediately following the expiration of the opportunity to cure where the recipient does not respond to the notice of violation required by section 7(b)(2). If the alleged violator does respond to the notice but is ultimately determined by the Commission to have not cured the violation, the Commission will then request repayment following that determination. What additional clarifications and/or rules are needed to implement these enforcement provisions?

### E. Cost-Benefit Analysis

60. The proposals in this Second Further Notice generally reflect mandates from the Secure Networks Act, and we have no discretion to ignore such congressional direction. To the extent that we are seeking comment on multiple possible options to implement any given mandate, we urge commenters, where possible, to include an assessment of relative costs and benefits for competing options. The proposals in this Second Further Notice are intended to, consistent with the Secure Networks Act, identify and provide guidance on which communications equipment and services the Secure Networks Act prohibit the use of Federal subsidies to purchase or maintain. We further seek detailed comments on the costs of the proposals in this Second Further Notice. What are the upfront and recurring costs associated with each? How will these costs vary according to the size of the provider of advanced communications service? The Commission already completed an Information Collection to determine the costs to ETCs to remove and replace Huawei and ZTE equipment and services.[104] How can we best incorporate this information into our cost-benefit analysis? What are the expected costs and benefits associated with each of these proposals to providers, end users, and any other relevant parties? We seek comment, generally, on the impact the proposed rules will have on small businesses and steps the Commission can take to mitigate the impact, if any, of these rules on those small businesses.

## V. PROCEDURAL MATTERS

61. *Ex Parte Presentations*. This proceeding is a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[105] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be

[101] *Id*. § 7(b)(1)(B), (D).

[102] *Id*. § 7(b)(2).

[103] *Id*. § 7(c).

[104] *See* FCC, Identifying Potentially Prohibited Communications Supply Chain Equipment and Services, www.fcc.gov/supplychain.

[105] 47 CFR §§ 1.1200 *et seq.*

found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

62. *Initial Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act, as amended (RFA),[106] the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities of the proposals addressed in this Notice of Proposed Rulemaking. The IRFA is set forth in Appendix B. Written public comments are requested on the IRFA. These comments must be filed in accordance with the same filing deadlines for comments on the Notice, and they should have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Notice, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration, in accordance with the RFA.[107]

63. *Paperwork Reduction Act Analysis.* This document contains proposed new information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

64. *Filing of Comments and Reply Comments*. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.[108] All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

[106] 5 U.S.C. § 603.

[107] *Id*. § 603(a).

[108] Due to the COVID-19 pandemic, the Commission closed its hand-delivery filing location at FCC Headquarters effective March 19, 2020. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Filing, Public Notice, DA 20-304 (rel. Mar. 19, 2020). As a result, hand or messenger delivered filings in response to this Notice of Proposed Rulemaking will not be accepted. Parties are encouraged to take full advantage of the Commission's various electronic filing systems for filing applicable documents. Except when the filer requests that materials be withheld from public inspection, any document may be submitted electronically through the Commission's ECFS. *See* 47 CFR § 1.49(f)(3). Persons that need to submit confidential filings to the Commission should follow the instructions provided in the Commission's March 31, 2020 public notice regarding the procedures for submission of confidential materials. *See FCC Provides Further Instructions Regarding Submission of Confidential Materials*, Public Notice, DA 20-361 (rel. Mar. 31, 2020).

- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington, DC 20554.

65. Comments and reply comments must include a short and concise summary of the substantive arguments raised in the pleading. Comments and reply comments must also comply with section 1.49 and all other applicable sections of the Commission's rules. We direct all interested parties to include the name of the filing party and the date of the filing on each page of their comments and reply comments. All parties are encouraged to use a table of contents, regardless of the length of their submission. We also strongly encourage parties to track the organization set forth in the Notice of Proposed Rulemaking in order to facilitate our internal review process.

66. *People with Disabilities*. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

67. *Contact Person*. For further information about this proceeding, contact Brian Cruikshank, FCC Wireline Competition Bureau, 445 12th St. SW, Washington, DC 20554, (202) 418-3623, brian.cruikshank@fcc.gov.

## VI. ORDERING CLAUSES

68. Accordingly, IT IS ORDERED that, pursuant to the authority contained in sections 4(i), 201(b), 214, 254, 303(r), 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 201(b), 214, 254, 303(r), 403 and 503, sections 2, 3, 5, and 7 of the Secure Networks Act, 47 U.S.C. §§ 1601, 1602, 1604, and 1606, and sections 1.1 and 1.412 of the Commission's rules, 47 CFR §§ 1.1 and 1.412, this Second Further Notice of Proposed Rulemaking IS ADOPTED.

69. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Second Further Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

70. IT IS FURTHER ORDERED that this Second Further Notice of Proposed Rulemaking will be EFFECTIVE upon publication in the Federal Register, with comment dates indicated therein.

71. IT IS FURTHER ORDERED that, pursuant to section 3 of the Secure Networks Act, 47 U.S.C. § 1602 and the authority contained in sections 1, 4(i), 201(b), 214, 254, 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 155(b), 155(c), 201(b), 214, 254, 303(r), and 403, and sections 1.2 and 54.9 of the Commission's rules, 47 CFR §§ 1.2 and 54.9, this Declaratory Ruling IS ADOPTED.

72. IT IS FURTHER ORDERED that the Declaratory Ruling is EFFECTIVE upon release.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

## APPENDIX A

## Draft Proposed Rules for Public Comment

**Part 1 – Practice and Procedure**

The authority citation for part 1 continues to read as follows:

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note, unless otherwise noted.

2. Add the following new subpart CC:

Subpart CC – Secure and Trusted Communications Networks

Authority: 47 U.S.C. chs. 5, 15.

**§ 1.40000 Purpose**

The purpose of this subpart is to set out the terms by which the Commission will publish and maintain the Covered List in accordance with the Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 133 Stat. 158.

**§ 1.40001 Definitions**

For purposes of this subpart:

(a) *Advanced communications service*. The term "advanced communications service" means high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction.

(b) *Appropriate national security agency*. The term "appropriate national security agency" means:

(1) The Department of Homeland Security;

(2) The Department of Defense;

(3) The Office of the Director of National Intelligence;

(4) The National Security Agency; and

(5) The Federal Bureau of Investigation.

(c) *Communications equipment or service*. The term "communications equipment or service" means any equipment or service that includes or uses electronic components that is essential to the provision of fixed or mobile advanced communications service with connection speeds of at least 200 kbps in either direction.

(d) *Covered communications equipment or service*. The term "covered communications equipment or service" means any communications equipment or service that is on the Covered List found in section 1.40002.

(e) *External determinations*. The term "external determination" means any determination from sources identified in § 1.40002(b)(1)(i)-(iv) that certain communications equipment or service poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(f) *Covered List.* The Covered List is a regularly updated list of covered communications equipment and services.

**§ 1.40002 Covered List**

(a) *Publication of the Covered List*. The Wireline Competition Bureau and the Public Safety and Homeland Security Bureaus shall publish the Covered List on the Commission's website. The Bureaus shall maintain the Covered List in accordance with section 1.40003.

(b) *Inclusion on the Covered List.* The Commission shall place on the Covered List any and all communications equipment and services that:

(1) is produced or provided by any entity if, based exclusively on the following determinations, such equipment or service produced or provided by such an entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons. The sources for these determinations are:

(i) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1222(a) of title 41, United States Code;

(ii) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain);

(iii) Equipment or service being covered 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

(iv) A specific determination made by an appropriate national security agency.

(2) and is capable of:

(i) Routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles;

(ii) Causing the networks of a provider of advanced communications services to be disrupted remotely; or

(iii) Otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.

**§ 1.40003 Updates to the Covered List**

(a) *Consultation with External Sources.* The Public Safety and Homeland Security Bureau shall monitor the status of external determinations in order to place additional communications equipment or services on the Covered List or to remove communications equipment and services from the Covered List.

(b) If an external determination regarding communications equipment or service on the Covered List is reversed, the Commission shall remove such equipment or service from the Covered List, except the Commission may not remove such equipment or service if any other of the sources identified in section 1.40002(b)(1)(i)-(iv) maintains an external determination supporting inclusion on the Covered List of such equipment or service.

3. Insert the following new section 1.7004:

**§ 1.7004 Reports on Covered Communications Equipment or Services**

(a) *Scope*. Each facilities-based provider of broadband connections to end users, as defined herein, shall submit an annual report to the Commission indicating whether the provider has purchased, rented, leased or otherwise obtained any covered communications equipment or service identified in the list published pursuant to section [X] of this chapter.

(b) *Definitions*.

(1) *Broadband connection.* A wired line, wireless channel, or satellite service that terminates at an end user location or mobile device and enables the end user to receive information from and/or send information to the internet at information transfer rates exceeding 200 kilobits per second (kbps) in at least one direction.

(2) *Facilities-based provider*. An entity is a facilities-based provider of a service if it supplies such service using facilities that satisfy any of the following criteria:

(i) Physical facilities that the entity owns and that terminate at the end-user premises;

(ii) Facilities that the entity has obtained the right to use from other entities, such as dark fiber or satellite transponder capacity, as part of its own network, or has obtained;

(iii) Unbundled network element (UNE) loops, special access lines, or other leased facilities that the entity uses to complete terminations to the end-user premises;

(iv) Wireless spectrum for which the entity holds a license or that the entity manages or has obtained the right to use via a spectrum leasing arrangement or comparable arrangement pursuant to subpart X of this Part (§§ 1.9001–1.9080); or

(v) Unlicensed spectrum.

(3) *End user*. A residential, business, institutional, or government entity that subscribes to a service, uses that service for its own purposes, and does not resell that service to other entities.

(c) *Contents of Report*. Each facilities-based provider of broadband service must:

(1) identify any covered communications equipment or service that is purchased, rented, leased or otherwise obtained on or after (i) August 14, 2018, in the case of any covered communications equipment or service on the initial list published pursuant to section [x] of this chapter; or (ii) within 60 days after the date on which the Commission places such equipment or service on the list required by section [x] of this chapter;

(2) provide details on the covered communications equipment or services in its network, including the type, location, date purchased, rented, leased or otherwise obtained, and any removal and replacement plans;

(3) provide a detailed justification as to why the facilities-based provider of broadband service purchased, rented, leased or otherwise obtained the covered communications equipment or service;

(4) provide information about whether any such covered communications equipment or service has subsequently been removed and replaced pursuant to Commission's reimbursement program contained in [Part 54, Subpart P];

(5) provide information about whether such provider plans to continue to purchase, rent, lease, or otherwise obtain, or install or use, such covered communications equipment or service and, if so, why; and

(6) include a certification as to the accuracy of the information reported by an appropriate official of the filer, along with the title of the certifying official.

(d) *Reporting Deadline*. Entities subject to this reporting requirement shall file initial reports within six months after the Office of Economics and Analytics issues a public notice announcing the availability of the new supply chain reporting platform. Thereafter, filers must submit reports once per year on or before June 30th, reporting information as of December 31st of the previous year.

(e) *Reporting Exception*. If a facilities-based provider of broadband service certifies to the Commission that such provider does not have any covered communications equipment or service in the network of such provider, such provider is not required to submit a report under this section after making such certification, unless such provider later purchases, rents, leases or otherwise obtains any covered communications equipment or service.

(f) *Authority to Update*. The Office of Economics and Analytics, in consultation with the Wireline Competition Bureau, the Wireless Telecommunications Bureau, the Public Safety and Homeland Security Bureau, and the International Bureau, may, consistent with these rules, implement any technical improvements, changes to the format and type of data submitted, or other clarifications to the report and its instructions.

**Part 54 — Universal Service**

3. The authority citation for part 54 is revised to read as follows:

Authority: 47 U.S.C. 151, 154(i), 155, 201, 205, 214, 219, 220, 229, 254, 303(r), 403, 1004, 1302, and 1601-1609, unless otherwise noted.

4. Insert the following new section 54.10:

**§ 54.10 Prohibition on Use of Certain Federal Subsidies**

(a) A Federal subsidy made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service may not be used to:

(1) purchase, rent, lease, or otherwise obtain any covered communications equipment or service; or

(2) maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.

(b) The term "covered communications equipment or service" is defined in section [x].

(c) The prohibition in paragraph (a) of this section applies with respect to any covered communications equipment or service beginning on the date that is 60 days after the date on which such equipment or service is placed on a published list pursuant to section [x] of this chapter. In the case of any covered communications equipment or service that is on the initial list published pursuant to section [x] of this chapter, such equipment or service shall be treated as being placed on the list on the date which such list is published.

5. Add new Subpart P – Secure and Trusted Communications Networks Reimbursement Program

**§ 54.1600 Purpose.**

The purpose of this subpart is to set out the terms by which providers of advanced communications service can seek and obtain reimbursements to replace covered communications equipment or services in accordance with the Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 133 Stat. 158.

**§ 54.1601 Reimbursement Program.**

Reserved.

**§ 54.1602 Enforcement.**

(a) In addition to the penalties provided under the Communications Act of 1934, as amended, and section 1.80 of this chapter, if a recipient in the Secure and Trusted Communications Networks Reimbursement Program (Program) violates the Secure and Trusted Communications Networks Act of 2019, Pub. L. 116-124, 133 Stat. 158, the Commission's rules implementing that statute, or the commitments made by the recipient in the application for reimbursement, the recipient:

(1) Shall repay to the Commission all reimbursement funds provided to the recipient under the Program;

(2) Shall be barred from further participation in the Program;

(3) Shall be referred to all appropriate law enforcement agencies or officials for further action under applicable criminal and civil law; and

(4) May be barred by the Commission from participation in other programs of the Commission, including the Federal universal service support programs established under section 254 of the Communications Act of 1934, as amended.

(b) *Notice and Opportunity to Cure*. The penalties described in paragraph (a) shall not apply to a recipient unless:

(1) the Commission, the Wireline Competition Bureau, or the Enforcement Bureau provides the recipient with notice of the violation; and

(2) the recipient fails to cure the violation within 180 days after the Commission or Bureau provides such notice.

(c) *Recovery of Funds*. The Commission will immediately take action to recover all reimbursement funds awarded to a recipient under the Program in any case in which such recipient is required to repay reimbursement funds under paragraph (a).

## APPENDIX B

## Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in the Second Further Notice of Proposed Rulemaking (FNPRM). Written comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments on the FNPRM provided on the first page of the item. The Commission will send a copy of the FNPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the FNPRM and IRFA (or summaries thereof) will be published in the Federal Register.[3]

### A. Need for, and Objectives of, the Proposed Rules

2. Consistent with our obligation to be responsible stewards of the public funds used in the Universal Service Fund (USF) programs and increasing concern about ensuring communications supply chain integrity, the FNPRM proposes and seeks comment on rules to implement sections 2, 3, 5, and 7 of the Secure Networks Act[4] and their applicability to the Commission's ongoing efforts to secure the communications supply chain.[5]

3. Specifically, the Commission proposes to establish the rules for the creation and maintenance of the Covered List, which will list communications equipment and services that providers of advanced communications services will be prohibited from using any Federal subsidy to purchase or maintain. The Commission also proposes to require advanced communications service providers to report their use of communications equipment and services published on the Covered List, and to adopt enforcement mechanisms the Commission may implement to as part of the reimbursement program established by section 4 of the Secure Networks Act.

### B. Legal Basis

4. The proposed action is authorized under sections 4(i), 201(b), 214, 254, 303(r), 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 201(b), 214, 254, 303(r), 403 and 503, sections 2, 3, 5, and 7 of the Secure Networks Act, 47 U.S.C. §§ 1601, 1602, 1604, and 1606.

### C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

5. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See* 5 U.S.C. § 603(a).

[3] *See id.*

[4] Pub. L. 116-124, 133 Stat. 158 (2020).

[5] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11429-32, paras. 5–17 (2019).

[6] 5 U.S.C. § 603(b)(3).

[7] 5 U.S.C. § 601(6).

same meaning as the term "small business concern" under the Small Business Act.[8] A small business concern is one that: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[9]

6. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[10] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[11] These types of small businesses represent 99.9% of all businesses in the United States which translates to 28.8 million businesses.[12]

7. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[13] Nationwide, as of Aug 2016, there were approximately 356,494 small organizations based on registration and tax data filed by nonprofits with the Internal Revenue Service (IRS).[14]

8. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[15] U.S. Census Bureau data from the 2017 Census of Governments[16] indicate that there were 90,075 local governmental jurisdictions consisting of general

[8] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in 15 U.S.C. § 632). Pursuant to the RFA, the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register." 5 U.S.C. § 601(3).

[9] *See* 15 U.S.C. § 632.

[10] *See* 5 U.S.C. § 601(3)–(6).

[11] *See* SBA, Office of Advocacy, "Frequently Asked Questions, Question 1 – What is a small business?" https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf (June 2016).

[12] *See* SBA, Office of Advocacy, "Frequently Asked Questions, Question 2- How many small businesses are there in the U.S.?" https://www.sba.gov/sites/default/files/advocacy/SB-FAQ-2016_WEB.pdf (June 2016).

[13] 5 U.S.C. § 601(4).

[14] Data from the Urban Institute, National Center for Charitable Statistics (NCCS) reporting on nonprofit organizations registered with the IRS was used to estimate the number of small organizations. Reports generated using the NCCS online database indicated that as of August 2016 there were 356,494 registered nonprofits with total revenues of less than $100,000. Of this number, 326,897 entities filed tax returns with 65,113 registered nonprofits reporting total revenues of $50,000 or less on the IRS Form 990-N for Small Exempt Organizations and 261,784 nonprofits reporting total revenues of $100,000 or less on some other version of the IRS Form 990 within 24 months of the August 2016 data release date. *See* http://nccsweb.urban.org/tablewiz/bmf.php where the report showing this data can be generated by selecting the following data fields: Show: "Registered Nonprofit Organizations"; By: "Total Revenue Level (years 1995, Aug to 2016, Aug)"; and For: "2016, Aug" then selecting "Show Results."

[15] 5 U.S.C. § 601(5).

[16] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

purpose governments and special purpose governments in the United States.[17] Of this number there were 36,931 general purpose governments (county[18], municipal and town or township[19]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[20] with enrollment populations of less than 50,000.[21] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[22]

9. Small entities potentially affected by the proposals herein include eligible schools and libraries, eligible rural non-profit and public health care providers, and the eligible service providers offering them services, including telecommunications service providers, Internet Service Providers (ISPs), and vendors of the services and equipment used for telecommunications and broadband networks.

### 1. Providers of Telecommunications and Other Services

#### a. Telecommunications Service Providers

10. *Incumbent Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[23] Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees.[24] U.S. Census Bureau data for

[17] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* Table 2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[18] *See* U.S. Census Bureau, 2017 Census of Governments - Organization, Table 5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[19] *See* U.S. Census Bureau, 2017 Census of Governments - Organization, Table 6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[20] *See* U.S. Census Bureau, 2017 Census of Governments - Organization, Table 10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10]. https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* Table 4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[21] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[22] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations Tables 5, 6, and 10.

[23] *See,* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[24] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

2012 indicate that 3,117 firms operated the entire year.[25] Of this total, 3,083 operated with fewer than 1,000 employees.[26] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[27] Of this total, an estimated 1,006 have 1,500 or fewer employees.[28] Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

11. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[29] The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[30] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.[31] Of that number, 3,083 operated with fewer than 1,000 employees.[32] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[33] Of this total, an estimated 317 have 1,500 or fewer employees.[34] Consequently, the Commission estimates that the majority of interexchange service providers are small entities

12. *Competitive Access Providers*. Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to competitive access services providers (CAPs). The closest applicable definition under the SBA rules is Wired Telecommunications Carriers and under the size standard, such a business is small if it has 1,500 or fewer employees.[35] U.S. Census Bureau data for

---

[25] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[26] *Id.*

[27] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*).

[28] *Id*.

[29] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[30] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[31] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[32] *Id*. The largest category provided by the census data is "1000 employees or more" and a more precise estimate for firms with fewer than 1,500 employees is not provided.

[33] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*). https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[34] *Id*.

[35] *See* 13 CFR § 121.201. The Wired Telecommunications Carrier category formerly used the NAICS code of 517110. As of 2017 the U.S. Census Bureau definition shows the NAICs code as 517311 for Wired Telecommunications Carriers. *See* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

2012 indicate that 3,117 firms operated for the entire year.[36] Of that number, 3,083 operated with fewer than 1,000 employees.[37] Consequently, the Commission estimates that most competitive access providers are small businesses that may be affected by our actions. According to Commission data in the *2010 Trends in Telephone Service Report*, 1,442 CAPs and competitive local exchange carriers (competitive LECs) reported that they were engaged in the provision of competitive local exchange services.[38] Of these 1,442 CAPs and competitive LECs, an estimated 1,256 have 1,500 or fewer employees and 186 have more than 1,500 employees.[39] Consequently, the Commission estimates that most providers of competitive exchange services are small businesses.

13. *Operator Service Providers (OSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The closest applicable NAICS Code category is Wired Telecommunications Carriers.[40] The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[41] U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year.[42] Of that number, 3,083 operated with fewer than 1,000 employees.[43] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[44] Of this total, an estimated 317 have 1,500 or fewer employees.[45] Consequently, the Commission estimates that the majority of OSPs are small entities.

14. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this

[36] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[37] *Id*.

[38] *See Trends in Telephone Service* at Table 5.3, page 5.5.

[39] *Id.*

[40] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[41] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[42] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[43] *Id*. The largest category provided by the census data is "1000 employees or more" and a more precise estimate for firms with fewer than 1,500 employees is not provided.

[44] *See Trends in Telephone Service*, Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*). https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[45] *Id*.

industry.[46] Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees.[47] 2012 Census Bureau data shows that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees.[48] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[49] Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees.[50] Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

15. *Toll Resellers*. The SBA has not developed a small business size standard specifically for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[51] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[52] Under that size standard, such a business is small if it has 1,500 or fewer employees.[53] The 2012 Census Bureau data show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[54] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[55] Of this total, an estimated 857 have 1,500 or fewer employees.[56] Consequently, the Commission estimates that the majority of toll resellers are small entities.

16. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including

---

[46] U.S. Census Bureau, *517911 Telecommunications Resellers,* https://www.census.gov/cgibin/sssd/naics/naicsrch?input=517911&search=2012+NAICS+Search&search=2012 (last visited Jan. 10, 2020).

[47] 13 CFR § 121.201, NAICS code 517911.

[48] U.S. Census Bureau, 2012 Economic Census, Subject Series: Information, "Establishment and Firm Size," NAICS code 517911.

[49] *See Trends in Telephone Service*, at Table 5.3.

[50] *See id*.

[51] U.S. Census Bureau, *517911 Telecommunications Resellers,* https://www.census.gov/cgibin/sssd/naics/naicsrch?input=517911&search=2012+NAICS+Search&search=2012 (last visited Jan. 10, 2020).

[52] 13 CFR § 121.201, NAICS code 517911.

[53] *Id.*

[54] U.S. Census Bureau, *American FactFinder*, https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table (last visited Jan. 10, 2020).

[55] *Trends in Telephone Service*, at tbl. 5.3.

[56] *Id.*

VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[57] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[58] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[59] Of this total, 3,083 operated with fewer than 1,000 employees.[60] Thus, under this size standard, the majority of firms in this industry can be considered small.

17. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[61] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[62] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[63] Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more.[64] Thus under this category and the associated size standard, the Commission estimates that the majority of Wireless Telecommunications Carriers (except Satellite) are small entities.

18. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions.[65] The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services.[66] Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500

---

[57] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[58] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[59] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.: 2012,* NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[60] *Id.* The largest category provided by the census data is "1000 employees or more" and a more precise estimate for firms with fewer than 1,500 employees is not provided.

[61] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite)",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517312&search=2017%20NAICS%20Search.

[62] *See* 13 CFR § 121.201, NAICS Code 517312 (previously 517210).

[63] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ5, *Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012*, NAICS Code 517210, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517210&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false&vintage=2012.

[64] *Id*. Available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees. The largest category provided is for firms with "1000 employees or more."

[65] *See* http://wireless.fcc.gov/uls. For the purposes of this IRFA, consistent with Commission practice for wireless services, the Commission estimates the number of licensees based on the number of unique FCC Registration Numbers.

employees.[67] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

19. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[68] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules.[69] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[70] Of this total, 299 firms had annual receipts of less than $25 million.[71] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

20. *All Other Telecommunications*. The **"**All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[72] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[73] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[74] The SBA has developed a small business size standard for "All Other Telecommunications", which consists of all such firms with annual receipts of $35 million or less.[75] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[76] Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49, 999,999.[77] Thus, the Commission estimates that the majority of

(Continued from previous page)

[66] *See* Federal Communications Commission, Wireline Competition Bureau, Industry Analysis and Technology Division, Trends in Telephone Service at Table 5.3 (Sept. 2010) (*Trends in Telephone Service*), https://apps.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf.

[67] *See id*.

[68] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications",* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517410&search=2017+NAICS+Search&search=2017.

[69] *See* 13 CFR § 121.201, NAICS Code 517410.

[70] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517410, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517410&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false&vintage=2012.

[71] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $35 million or less.

[72] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=517919&search=2017+NAICS+Search&search=2017.

[73] *Id.*

[74] *Id*.

[75] *See* 13 CFR § 121.201, NAICS Code 517919.

[76] *See* U.S. Census Bureau, *2012 Economic Census of the United States*, Table ID: EC1251SSSZ4, *Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the U.S.: 2012*, NAICS Code 517919, https://data.census.gov/cedsci/table?text=EC1251SSSZ4&n=517919&tid=ECNSIZE2012.EC1251SSSZ4&hidePreview=false.

[77] *Id.*

"All Other Telecommunications" firms potentially affected by our action can be considered small.

### b. Internet Service Providers

21. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications infrastructure fall in the category of Wired Telecommunication Carriers.[78] Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies.[79] The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees.[80] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year.[81] Of this total, 3,083 operated with fewer than 1,000 employees.[82] Consequently, under this size standard the majority of firms in this industry can be considered small..

## D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

22. The FNPRM proposes rules that establish a Covered List of communications equipment and services that advanced communications providers are prohibited from using federal subsidies administered by the Commission to purchase or maintain. The FNPRM also proposes rules to create a reporting requirement for advanced communications providers to identify whether they use or maintain any equipment or services on the Covered List in their networks. We seek comment on this proposal, and its likely costs and benefits, as well as on alternative approaches and any other steps we should consider taking.

## E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

23. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[83]

24. In compliance with the Secure Networks Act, the FNPRM specifically proposes to establish the Covered List, reporting requirements for advanced communications providers, and enforcement mechanisms for violations of the prohibition on the use of federal subsidies to purchase or

---

[78] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers"*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[79] *Id.*

[80] *See* 13 CFR § 121.201, NAICS Code 517311 (previously 517110).

[81] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table ID: EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms for the U.S.*: *2012*, NAICS Code 517110, https://data.census.gov/cedsci/table?text=EC1251SSSZ5&n=517110&tid=ECNSIZE2012.EC1251SSSZ5&hidePreview=false.

[82] *Id.* The largest category provided by the census data is "1000 employees or more" and a more precise estimate for firms with fewer than 1,500 employees is not provided.

[83] *See* 5 U.S.C. § 603(c).

maintain communications equipment and services on the Covered List.

25. We expect to take into account the economic impact on small entities, as identified in comments filed in response to the FNPRM and this IRFA, in reaching our final conclusions and promulgating rules in this proceeding. The FNPRM generally seeks comment on how to adopt enacted legislation that mandates action by the Commission and seeks specific comment on how to mitigate the impact on small entities.

**F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules**

26. None.

**STATEMENT OF**
**CHAIRMAN AJIT PAI**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

National security experts have warned that when companies are beholden to foreign governments with interests adverse to the United States, their products and services can threaten our country. This is certainly the case with the Chinese telecommunications equipment manufacturers Huawei and ZTE. As Lieutenant General and former National Security Advisor H.R. McMaster recently explained in The Atlantic, China "use[s] . . . major telecommunications companies to control communications networks and the [I]nternet overseas."

This is not surprising. Huawei and ZTE each have close ties to the Chinese Communist Party and China's military, and both companies are broadly subject to Chinese law obligating them to cooperate with the country's intelligence services. With respect to Huawei, McMaster writes, "There should no longer be any dispute concerning the need to defend against . . . Huawei and its role in China's security apparatus." In light of the "incontrovertible evidence of the grave national-security danger associated with a wide array of Huawei's telecommunications equipment," he advises that a policy priority for the United States and its allies should be "the development of infrastructure, particularly 5G communications, to form trusted networks that protect sensitive and proprietary data."

At the FCC, we couldn't agree more. That's why, last fall, the Commission unanimously adopted a ban on the use of universal service support to purchase, obtain, or maintain any equipment or services from companies posing a national security threat to communications networks or the communications supply chain. And last month, the FCC's Public Safety and Homeland Security Bureau formally designated Huawei and ZTE as covered companies for purposes of our November 2019 ban. As a result, the FCC's $8.3 billion a year Universal Service Fund (USF) can no longer be used to underwrite these suppliers.

Today, we take additional steps to protect America's communications networks from national security threats. Specifically, we integrate provisions of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which was enacted in March 2020, into our existing supply chain rulemaking proceeding. We start with a Declaratory Ruling in which we determine that we've already fulfilled one of our new statutory obligations. In particular, we find that by adopting our November 2019 ban on USF support for equipment and services produced or provided by companies that pose a national security threat, we have substantially met our obligation under the Secure Networks Act to prohibit the use of federal subsidies for covered communications equipment and services.

We also adopt a Second Further Notice of Proposed Rulemaking to seek public input on implementing various other parts of the Secure Networks Act. First, we propose ways to create and maintain the list of covered communications equipment and services required by the statute. Second, we propose to ban the use of federal subsidies, including USF funding, for any communications equipment or services placed on this list. Third, we propose to require all providers of advanced communications services to report on whether they use any covered communications equipment or services. Finally, we propose rules to prevent waste, fraud, and abuse in the reimbursement program to remove and replace insecure equipment that Congress has mandated in the Secure Networks Act. We sought comment on this reimbursement program in April 2020, and I hope that Congress will act quickly to appropriate funding for it. Indeed, last fall, we estimated that a removal-and-replacement program could cost up to $2 billion, so this would be a critical step forward.

For their outstanding work to help secure our nation's communications infrastructure, I'd like to thank the following Commission staff: Pam Arluk, Brian Cruikshank, Justin Faulb, Trent Harkrader, Billy Layton, Kris Monteith, Ramesh Nagarajan, Ryan Palmer, and Morgan Reeds of the Wireline Competition Bureau; Malena Barzilai, Ashley Boizelle, Mike Carlson, Tom Johnson, Doug Klein, Rick

Mallen, and Bill Richardson of the Office of General Counsel; Tanner Hinkel, Ken Lynch, Alec MacDonnell, and Steve Rosenberg of the Office of Economics and Analytics; Jeff Goldthorp, Deb Jordan, Nikki McGinnis, Saswat Misra, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Chrysanthos Chrysanthou, Martin Doczkat, Michael Ha, Ira Keltz, Aspa Paroutsas, and Sean Yun of the Office of Engineering and Technology; and Maura McGowan of the Office of Communications Business Opportunities.

I'd also like to thank the bipartisan group of Representatives and Senators who led efforts to pass the Secure Networks Act, including Chairman Wicker, Senator Warner, Chairman Pallone, and Ranking Member Walden. Thanks as well to Senators Cotton and Rubio for highlighting this issue. All of these efforts are helping make our communications networks safer, and I look forward to continuing to work with them on this national priority.

**STATEMENT OF**
**COMMISSIONER MICHAEL O'RIELLY**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

Maintaining the security and integrity of our communications infrastructure is of paramount importance. Over the past year or so, it rightfully has been a heightened priority of the FCC, Administration, and Congress to protect our communications networks from external threats, such as incursions by the Chinese Communist government through the "companies" they control.

For instance, the Commission prohibited certain equipment from being supported by Universal Service Funds, designated Huawei and ZTE as potential threats to our infrastructure, and sought comment on ripping and replacing certain equipment from all networks, among other actions. The President has signed an executive order providing the Department of Commerce with the authority to prohibit transactions when they would pose a threat to U.S. infrastructure or national security. Congress has passed multiple bills addressing Huawei and ZTE and created the Federal Acquisition Security Council to lead a government-wide effort to evaluate threats posed by communications services and equipment. Most recently, the Secure 5G and Beyond Act, authored by Senators Cornyn, Burr, and Warner, was signed into law to keep 5G networks secure from foreign interference. I appreciate that all of these efforts have brought added attention to and provided much needed guidance on these important issues.

Most relevant to today's item is the Secure and Trusted Communications Networks Act, which incorporates and expands upon the 2019 actions taken by the Commission. The item declares that the FCC's actions to prohibit USF funds from being spent on Huawei and ZTE equipment is consistent with and satisfies certain provisions of the Act, and it seeks comment on how to implement the remainder of the law. As always, I will follow Congressional direction and fully support our action today. Many thanks to Representatives Pallone, Walden, Matsui, and Guthrie, along with Senators Wicker, Thune, Cotton, Warner, Markey, and Sullivan, for ushering this bill through Congress.

I do have one area of concern, however, that is related to today's item. With all of the activity previously described, there are multiple conversations taking place about what equipment and services pose an actual risk to our national security. This is an important, but not easy, undertaking and involves some necessary line drawing. The FCC used a very broad definition in 2019, and, based on our definition, certain entities reported to the FCC whether they had covered equipment in their networks. Other federal agencies, however, do not appear to be taking the exact same approach. Given the lack of consensus on what equipment and services pose a national security risk, we should take a step back and delay any publication of the list of companies that reported covered equipment under our definition.

Publicly exposing companies, which did not do anything wrong at the time they purchased their equipment, and potentially causing substantial financial harm should only be considered as a necessary step if their equipment is ultimately determined to pose a true threat. This is not to say that the Commission erred in requesting this data, as sometimes there is a first mover disadvantage, or that this information does not provide the Commission with useful insights. But, in order to provide certainty to industry and clarity to Americans about the actual risks of using certain networks, all involved federal agencies should be on the same page regarding what equipment and services could harm our national security before prematurely publishing a list of names, which, in the end, may include companies whose equipment ultimately is determined not to cause concern.

I thank the Chairman for bringing this important item to a vote. I approve.

**STATEMENT OF**
**COMMISSIONER BRENDAN CARR**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

*The rule of law. Clean and light-handed government. The values of a free society. The beginnings of representative government and democratic accountability. . . . Hong Kong's values are decent values. They are universal values. They are the values of the future in Asia as elsewhere, a future in which the happiest and the richest communities, and the most confident and the most stable too, will be those that best combine political liberty and economic freedom as we do here today. . . . Now, Hong Kong people are to run Hong Kong. That is the promise. And that is the unshakeable destiny*.

— Chris Patten, the last Governor of Hong Kong, June 30, 1997, at the Handover Ceremony from British rule to the People's Republic of China

For the next 20 years, that destiny did not shake. Hong Kong prospered as a free, self-governing community: its judiciary independent, its markets open. And like Taiwan, it served as a potent reminder to Mainland China of what could be.

"One country, two systems" was guaranteed by law. Margaret Thatcher and Deng Xiaoping negotiated in writing 50 years of freedom for Hong Kong. It was the reformers' bet that the example of Hong Kong would inspire mainland Chinese to agitate for changes to their own government. And so Article V of Hong Kong's new constitution provided that "the previous capitalist system and way of life shall remain unchanged" for five decades.

But the reformers' hope for Hong Kong was not based on paper alone. By 1997, Hong Kong already had grown into a global financial center to rival New York or London. It was an international air and cargo hub. It was itself a member of the WTO, several years preceding China's admission. China's regime looked longingly at Hong Kong's success and had created the Shenzhen Special Economic Zone bordering Hong Kong to spur manufacturing and leverage the city's advantages.

In short, the theory was: Hong Kong would be too rich to fail. China had too much invested in Hong Kong's economic success spilling into the rest of China to risk a political clampdown.

Yet Beijing now has taken that risk. Two weeks ago, it imposed on Hong Kong a new security law, making it a crime to abet criticism of Beijing, stripping residents of their broad right to trial by jury, and easing extradition to the mainland, where durable rights against the government are rare. According to Hong Kong police, the very first arrest made under the new security law was for a man who had the audacity to unfurl a Hong Kong independence flag in public.

The U.S. government has been examining Huawei, ZTE, and other telecom suppliers with close ties to the Communist regime in China. We have cataloged a pattern of misdirected traffic, software vulnerabilities, and suspicious deployments. We have examined China's National Intelligence Law, which compels companies' aid in advancing a "comprehensive concept of national security." And we have observed the due process China's judiciary offers—and the conviction rate it delivers for the regime.

Huawei's and others' response, again and again, comes back to this: Why would we, successful international suppliers of telecom, risk our reputations and our profits by making our products insecure? And why would the Chinese regime risk its years of investment in these companies for a leg up on spying?

They were meant to be rhetorical questions. They can't be after Hong Kong.

If "one country, two systems" has revealed itself as a sham in Hong Kong, we cannot expect "one company, two systems" to fare any better at Huawei.

It's therefore right that Congress acted to protect our security against these threats, and through this order, again, so do we.

I thank the Wireline Competition Bureau and all of the Commission's staff for their work on this item. It has my support.

**STATEMENT OF**
**COMMISSIONER JESSICA ROSENWORCEL**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

We live in a world gone wireless. Our future will be built on 5G infrastructure. So we need to ensure that infrastructure is safe—and that begins with keeping insecure equipment out of our networks.

Today the Federal Communications Commission helps do just that by acting at the direction of Congress to implement the Secure and Trusted Communications Networks Act. This law prohibits the use of public funds to obtain communications equipment or services from a company that poses a national security risk. In addition, it requires the FCC to maintain a list of "covered communications equipment or services" that could undermine our national security and it authorizes a program to reimburse the cost of replacing prohibited equipment.

But take note, because this is only one action in a series taken by this agency to keep insecure equipment out of our nation's communications networks. Two years ago, the FCC first sought comment on supply chain issues and proposed a rule to prohibit the use of universal service funds to purchase equipment and services from providers that may pose a security risk. Last year, we adopted this rule. Then we started an information collection to survey where insecure equipment is in our networks and estimate the cost to remove it. We also denied an application from China Mobile to enter our markets and put four other similarly situated companies on notice they could share the same fate. Last month we designated two Chinese companies—Huawei and ZTE—as national security threats because the evidence suggests the Chinese government could exert control over them. It is clear the world is watching. Because just this week the United Kingdom announced it, too, will bar its networks from using 5G equipment made by untrusted providers.

In the instant decision, we find that our efforts last year prohibiting the use of universal service funds to support the purchase of insecure equipment and services largely satisfy our obligations under Section 3 of the Secure and Trusted Communications Networks Act. Then in the rulemaking we seek comment on how to implement the remaining aspects of this law. Over time, I hope we can do more to harmonize the processes we established last year with those required in this new law. I also hope we can explore how existing law—from the Communications Act to the Communications Assistance for Law Enforcement Act—can bolster those efforts. So today's decision and rulemaking has my support.

But let's not stop here. Because there is more we can do to secure our 5G future. There is more we can do to power the future of innovation. There is more we can do to make sure the United States has a fighting chance at leading in what comes next.

That begins with fixing our obvious missteps. Those include suspending new work visas for a wide variety of technology jobs and deterring foreign students from studying and staying on our shores—something the President of the Massachusetts Institute of Technology has said fuels our "persistent advantage in scientific creativity." Likewise, we need to be mindful how increased consolidation in our economy impacts what innovations make it to market and get the opportunity to change our world.

Closer to home, we need the FCC to do more than just ban the presence of Chinese companies. Because this is not about retribution. It is about building a better future. If we want to ensure no equipment provider can undermine our communications, we need the United States to spur a new and more innovative and diverse ecosystem of secure equipment and equipment providers. I think the FCC can help do that.

A year ago, at a gathering of Mobile World Congress Americas, I was the first to call on the FCC to help develop a more secure communications future by supporting open radio access networks—or open RAN. The RAN is the part of the network that sits between your device and the network core. It is the

most expensive and restrictive part of the network today. All major components of a RAN have to come from the same vendor—there is no way to mix and match.

When I offered this idea, no companies based in the United States were manufacturing 5G equipment for this part of our networks—thanks in part to a long history of consolidation in the sector. Meanwhile, Chinese companies were selling nearly half of all global RAN gear. The security risks inherent in this state of affairs are easy to understand.

So I suggested that we do something to reverse these trends. I suggested that if we can unlock the RAN by virtualizing this part of our network, we could help spur a market for more secure 5G equipment. We could expand the number of suppliers, promote the long-term viability of the 5G supply chain, and prevent growing dependence on Chinese vendors. Even better, this effort could push the market for 5G equipment to the sectors where the United States is strongest: in software and semiconductors.

I got the chance to talk more about this when I testified before the Senate Committees on Homeland Security and Government Affairs and Commerce, Science, and Transportation. In recent months, it has garnered support from my colleagues at the FCC too. It is a recurring theme in comments to the National Telecommunications and Information Administration on the National Strategy to Secure 5G Implementation Plan. And it has been embraced by more than 30 companies that have joined the Open RAN Policy Coalition.

This is progress. But here is what we need to do next.

First, we need a whole-of-government approach to advancing open RAN in the United States. Right now, we don't have it. The Attorney General recently called this effort "just pie in the sky." He's not right. It may be audacious, but that's exactly why the United States needs to lead. Yet there are reports that the Department of State wants a watered-down version of the open RAN concept. This is troubling. Across the board we need a more cohesive government-wide 5G strategy, especially with open RAN.

Second, we need to develop testbeds in the United States that bring together a mix of stakeholders interested in developing and promoting open RAN. As I've said before, the FCC can build this into our ongoing effort to authorize city-wide 5G testbeds in New York and Salt Lake City. But to date we haven't done so. In the meantime, the United Kingdom is working on 5G testbeds to support open RAN, the European Union is boosting investment in 5G equipment innovation, and a Japanese company has already deployed a commercial mobile network using open RAN. Plus, the Department of Defense is working on 5G testbeds that will include open RAN architectures. I think the FCC should support testbeds for the commercial development of this capability, too.

Third, the we need to task the FCC's Communications Security, Reliability, and Interoperability Council with identifying impediments to open RAN development in the United States and what new efforts can be undertaken to support secure and interoperable equipment. It already has a charter to consider security risks in emerging 5G networks. We need to expand it to explore this technology. Similarly, when the FCC participates in standards-setting bodies like 3GPP and the Alliance for Telecommunications Industry Solutions, we should consider how we can support the goals of openness and interoperability.

Fourth, we need resources to make this all happen. For starters, we need an appropriation from Congress for the reimbursement program created by the Secure and Trusted Communications Networks Act. But solving our security challenges in the present is not enough. So I hope Congress proceeds with the Utilizing Strategic Allied Telecommunications Act, which would fund research and development for a secure wireless supply chain. The odds are good. Because just this week the Energy and Commerce Committee advanced this legislation to the full House of Representatives. In addition, elements of the Senate version of this bill have been included in the Intelligence Authorization Act, demonstrating just how powerful these matters are for national security both at home and abroad.

All of these efforts would help our supply chain challenges today and more importantly, assist with the development of a more secure and innovative future. We need to remember we cannot limit our focus to keeping untrusted companies and Chinese equipment out of our networks. We need a vibrant and diverse set of trusted equipment and companies in their place, and the United States should help lead the development of this new communications ecosystem. The most important thing is that we get started right now.

**STATEMENT OF**
**COMMISSIONER GEOFFREY STARKS**

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89.

Network security is national security. As we confront foreign cyberthreats to our economy, our elections, and even our response to the COVID-19 pandemic, these words have never been truer. Certain foreign telecommunications equipment companies rapidly vaulted themselves into a leading global position, as well as a foothold in U.S. networks. Today's decision is another step by this Commission toward eliminating untrustworthy equipment in our networks. But we need a broader, more cohesive plan to develop and support alternatives that both replace existing equipment and position us to better compete in the future.

Through its "Made in China 2025" strategy, the Chinese government has provided critical support to Huawei and ZTE that artificially lowered their prices, assisted in their research and product development, and undercut international competition. This was not free-market competition, but part of a strategy to leverage economic power into geopolitical dominance. Through this unfair advantage, the equipment produced by these corporations has become pervasive around the world. At first glance, these actions could be considered simple economic gamesmanship—a tactical ploy to become the dominant telecom equipment ecosystem, set manufacturing standards, and "win" the race to 5G.

But as we've established in this proceeding, such a view overlooks the other half of the bargain between these foreign competitors and their government. According to our intelligence agencies, in exchange for this subsidization, corporations like Huawei and ZTE have siphoned data, allowed backdoor access to state agencies, and enabled functionality for network disruption. As a result, the technological foundation of our communications networks has been weaponized.

But the tide is turning, as evidenced by this week's decision by the UK government to ban Huawei from its 5G networks. Here in the United States, last year I called for the FCC to find each piece of untrustworthy equipment in our networks, to fix the problem by instituting a replacement program, and to fund the replacement of this equipment. My find it, fix it, fund it proposal was a comprehensive and unequivocal response—untrustworthy equipment that threatens our data privacy and network security cannot be managed or tolerated in any form.

Today, we largely codify that response and integrate it with the provisions of the Secure and Trusted Communications Networks Act. Universal Service funds will no longer be used to finance commerce with bad-faith actors, and we begin proceedings to replace the untrustworthy equipment in our networks.

As our world becomes even more interconnected, the FCC has a critical role to play in protecting that security. The Commission must be proactive, not reactive, in national security measures in order to avoid problems like untrustworthy network equipment in the future. And though we've done much, much remains to be done. A few additional thoughts.

First, as I've called for before, we need to create an FCC National Security Task Force. The Commission currently reviews national security issues on a distributed basis among the various bureaus. For example, the International Bureau refers applications for Section 214 authorizations involving foreign ownership to "Team Telecom" for national security review. The Public Safety and Homeland Security Bureau participates in the National Security Council's NSPM-4 process. And the Wireline Competition and Wireless Telecommunications Bureaus consider national security in license transfers and number portability matters.

This distributed structure makes internal coordination challenging and risks inconsistent treatment of national security issues between different bureaus. These issues are not going to diminish. Quite the opposite, in fact, as I expect that the Commission will continue to see an increase in the number and

complexity of issues that will touch on national security. Security issues surrounding Team Telecom, CFIUS, 214 authorizations, numbering and so forth are becoming more common. We must be more intentional than ever to ensure that the whole of the FCC is more coordinated, more deliberative, and more collaborative. The FCC should issue a Public Notice creating a National Security Task Force, like other task forces established by the FCC in the past.

Second, as we proceed, we must promote equipment supplier diversity and level the competitive playing field so we have options for replacing this equipment and avoid replicating this situation in the future. We must also champion new innovations that can ensure a more robust, reliable communications network. This includes serious consideration of Open RAN (O-RAN) technology solutions for replacing untrustworthy equipment and updating our communications infrastructure more generally.

O-RAN is promising because it enables a single distributed system of interoperable hardware. With interoperability, individual components can be interchanged without replacing whole systems. This granular approach reduces the barriers to entry for radio access network component vendors, particularly small-scale or specialized suppliers, and presents an opportunity for American companies to reassert their role in the communications equipment sector. A new competitive and diverse market of vendors would allow each carrier to establish the most innovative and appropriate combination of network components for its needs, rather than purchasing equipment on a one-size-fits-all basis.

O-RAN emphasizes software defined functions through open interfaces and a cloud hierarchy. Both features accommodate innovation and allow for a more robust and responsive network environment. For example, scaled design improvements, as well as updates to network systems, may occur at lower costs and faster timetables. This responsiveness will allow carriers to harmoniously merge legacy and next generation wireless systems as they replace older or untrustworthy equipment.

And we know that O-RAN isn't—as some have suggested—"pie in the sky." It is available right now. DISH Network recently selected network software provider Mavenir to deliver cloud-native O-RAN software to buildout its 5G wireless networks.

The scope of our item today focuses on how we "rip" and not on how we "replace." But in reality, the two go together, by necessity. We must do some deep and proactive thinking on the best policies to effectuate our goals of promoting secure telecommunications networks that benefit our shared future and get the best value for American tax-payer dollars. So here's a new idea. In future items, I recommend we explore that each "rip-and-replace" carrier rebuilding its network be required to consider solutions offered by an O-RAN provider. That would achieve many of our goals, including encouraging global competition with Huawei, capitalizing on U.S. software advantages, accelerating the development of O-RAN as a product-model and a business-case, and allowing for alternative vendors to enter the market and offer specific network solutions. If American tax-payer dollars are going to rebuild these networks, Americans should get the best value and the most benefit.

Third, even as we discuss potential alternatives to the untrustworthy equipment in our communications networks, we still lack the funding necessary to remove and replace that equipment. Last year, in meetings across the country, small carriers repeatedly told me about their need for help to replace equipment that they bought legally and in good faith. To their credit, many of these same carriers have experienced substantial losses as a result of honoring the Keep Americans Connected Pledge, further weakening their ability to replace this equipment on their own. We must coordinate with Congress to ensure that sufficient funds are appropriated, and that a remedy can be provided quickly and responsibly.

Our actions today are swift and clear, but much work lies ahead. We must join with policymakers both here and abroad to address not only the challenge of untrustworthy equipment already in our networks but how to respond to adversary states' attempts to leverage market dominance into geopolitical influence. Experience has taught us that we can counter these efforts only by identifying a realistic alternative. Let's get to work.

Thank you to the staff of the Wireline Competition Bureau for their work on this item.