6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 1 and 54

[WC Docket No. 18-89; FCC 20-99; FRS 16964]

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs

AGENCY: Federal Communications Commission

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) takes further steps to protect the nation's communications networks from potential security threats as the Commission integrates provisions of the recently enacted Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act) into its existing supply chain rulemaking proceeding. The Commission seeks comment on proposals to implement further Congressional direction in the Secure Networks Act.

DATES: Comments are due on or before **[INSERT DATE 21 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due on or before **[INSERT DATE 35 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Pursuant to §§ 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 and reply 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. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number. Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-

class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- 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.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.
- During the time the Commission's building is closed to the general public and until further notice, if more than one docket or rulemaking number appears in the caption of a proceeding, paper filers need not submit two additional copies for each additional docket or rulemaking number; an original and one copy are sufficient.

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 § 1.49 and all other applicable sections of the Commission's rules. The Commission directs 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. The Commission also strongly encourages parties to track the organization set forth in the Further Notice in order to facilitate its internal review process.

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).

FOR FURTHER INFORMATION CONTACT: For further information, please contact Brian Cruikshank, Telecommunications Access Policy Division, Wireline Competition Bureau, at Brian.Cruikshank@fcc.gov or (202) 418-7400.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Second Further Notice of Proposed Rulemaking (Further Notice) in WC Docket No. 18-89, adopted July 16, 2020 and released July 17, 2020. Due to the COVID-19 pandemic, the Commission's headquarters will be closed to the general public until further notice. The full text of this document is available at the following Internet address: https://www.fcc.gov/document/implementing-secure-networks-act-0. The Declaratory Ruling that was adopted concurrently with this Further Notice will be published elsewhere in the *Federal Register*.

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 the Commission safeguards 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, the Commission 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. The Commission also initially designated Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of this rule, and it 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. The Commission takes further steps to protect the nation's communications networks

from potential security threats as it integrates provisions of the recently enacted Secure Networks Act into the Commission's existing supply chain rulemaking proceeding. The Commission seeks comment on proposals to implement further Congressional direction in the Secure Networks Act.

II. SECOND FURTHER NOTICE OF PROPOSED RULEMAKING

4. The concurrently adopted Declaratory Ruling finds that the *2019 Supply Chain Order*, 85 FR 230, January 3, 2020, satisfies the Secure Networks Act's requirement that the Commission prohibit the use of funds for covered equipment and services. The Commission now seeks 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. As required by section 2, the Commission proposes 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, the Commission proposes 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.

5. After the Commission has 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 the USF, to purchase or maintain communications equipment and services listed pursuant to section 2. The Commission seeks comment on this view.

6. As an initial matter, the Commission seeks 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." 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."

7. The Commission proposes 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. The Commission believes 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. The Commission seeks comment on this interpretation.

8. The Commission also proposes 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. The Commission thus believes its 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.

9. The Commission recognizes the greater than 200 kbps reporting threshold reflects historical considerations as to speeds needed to provide advanced telecommunications capability. 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." 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." 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 security. The Commission seeks comment on this interpretation and any alternatives.

10. 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). 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" 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." *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). The Commission seeks comment on each part in turn.

11. 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. The Commission believes 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. The Commission seeks comment on this interpretation.

12. 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."

13. The Secure Networks Act defines "executive branch interagency body" as "an interagency body established in the Executive Branch." 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. The Commission believes 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. The Commission seeks comment on this view and asks 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? The Commission also seeks comment on the process and procedures it should use to incorporate executive branch interagency body determinations into the Covered List.

14. 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. In November 2019, the Department of Commerce commenced a rulemaking to implement Executive Order No. 13873. The Commission seeks comment on the process and procedures it should use to incorporate Department of Commerce external determinations into the Covered List.

15. The Commission is also required to incorporate into the Covered List equipment or services identified in section 889(f)(3) of the 2019 NDAA. The Commission seeks 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." 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 China]."

16. The Commission seeks comment on how it 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. The Commission reads 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 the Commission reads 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. The Commission seeks 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 the Commission interpret section 889(f)(3)(D) and any subsequent designations made by the Department of Defense? What other considerations are relevant to its interpretation of section 889(f)(3)?

17. 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. 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. The Commission interprets 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. The Commission also seeks comment on the process and procedures it should use to incorporate their determinations into the Covered List.

18. The Commission seeks comment on what constitutes a specific determination that

triggers its obligations under section 2(b)(1). Do the entities listed in section 2(c) have different processes to identify the equipment and services that the Commission 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. Should the Commission 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 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?

19. Relatedly, the Commission seeks comment generally on the mechanics of using these determinations to publish the Covered List. The Commission expects that any determinations covered under sections 2(c) will be publicly released by the original decisionmaker. If such a determination is public, the Commission does not believe it must issue any notice regarding their receipt of this determination. The Commission seeks 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. In order to meet this deadline, by what date does the Commission need to receive the external determinations? Should the Commission affirmatively solicit these determinations from other agencies and, if so, how? Are there any other procedures the Commission should consider to comply with section 2(c) of the Secure

Networks Act?

20. 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" 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."

21. The Commission starts 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)?

22. The Commission resolves 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, the Commission 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, the Commission

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

23. 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 or ZTE (or any subsidiary or affiliate of such entities)." When an external source identifies classes or categories of equipment or services as part of its external determination, the Commission believes 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." As such, the Covered List would include "Telecommunications equipment produced by Huawei or ZTE 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." The Commission seeks comment on this proposal. In turn, the Commission seeks comment on how it should define "capable" for purposes of section 2(b)(2) of the Secure Networks Act. The Commission believes "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. The Commission seeks 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)?

24. The Commission seeks comment on alternatives to its lead proposal. For example, once the Commission receives an external determination that communications equipment or services pose an unacceptable security risk, should the Commission 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 the Commission permissibly find that equipment is not "capable" of posing an unacceptable risk even if it must "exclusively" rely on a section 2(c) source to determine that it does actually pose such a risk? Must the Commission 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? The Commission seeks comment on other potential methods of interpreting and complying with section 2 of the Secure Networks Act and their costs and benefits.

25. Finally, regardless of how the Commission interprets the interplay of section 2(b)'s various provisions, it seeks 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. How can the Commission provide interested parties adequate opportunities to demonstrate that specific equipment or services are or are not included on the

Covered List while meeting its obligations under the Secure Networks Act?

26. 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. 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. 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. The Commission reads the language of section 2(d) to be mandatory—precluding it from altering the list beyond the specific updates (all tied to changes in section 2(c) determinations) required by its terms. The Commission seeks comment on this interpretation. The Commission also seeks 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.

27. Consistent with the Secure Networks Act, which establishes no notice period before the publication of the Covered List, the Commission proposes to publish the Covered List without first seeking public comment on the contents. The Commission notes 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. The Commission seeks comment on this proposal.

28. In the concurrently adopted Declaratory Ruling, the Commission found that the prohibition adopted in § 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 § 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." 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.

29. The Commission proposes and seeks comment on the designation of covered communications equipment and services on the Covered List. If the Commission's proposal here is adopted, it 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, the Commission proposes a new rule, independent of the § 54.9 prohibition, that would prohibit, going forward, the use of federal subsidies made available through a program administered by the Commission to purchase, rent, lease, otherwise obtain, or maintain any covered communications equipment and services identified and published on the Covered List. The Commission proposes 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. The Commission seeks 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 § 54.9.

30. As discussed in the concurrently adopted Declaratory Ruling, the Commission reads 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. The Commission seeks comment on this proposal. The Commission believes that applying this prohibition to USF programs furthers its 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 its 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. The Commission seeks comment on this approach.

31. The Commission seeks 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. The Commission specifically seeks comment on whether the Secure Networks Act, which states that the prohibition shall apply 60 days after the date on which it places a service or piece of equipment on the Covered List, permits the Commission to grandfather any such arrangements. If the Commission does grandfather contracts, should it only grandfather unexpired annual or multiyear contracts, or also grandfather one-year contracts with voluntary extensions? The Commission notes that in the *2019 Supply Chain Order*, it declined to grandfather existing contracts, finding that "[e]xempting existing multiyear contracts would negate the purpose behind its rule and allow federal funds to be used to perpetuate existing security risks to communications networks and the communications supply chain." To what extent would the Commission's adoption of the proposed rule trigger any change-of-law provisions?

32. Are there other practical issues raised by the Commission's proposals that it should address in implementing this proposed rule? Would section 3, any other section of the Secure Networks Act, or the Secure Networks Act as a whole provide us independent authority to require ETCs or other providers to remove and replace equipment on the Covered List?

33. 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." 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.

34. 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. 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.

35. While the Commission recently conducted an information collection to better understand the extent of Huawei and ZTE equipment in our communications networks, it recognizes the annual reporting requirement contained in section 5 goes beyond the scope and frequency of that collection. The Commission 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. Accordingly, the collection would not satisfy section 5 of the Secure Networks Act absent significant modification.

36. The Commission therefore proposes and seeks comment on a new information collection requirement to implement section 5. Specifically, the Commission proposes 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, the Commission proposes 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. The Commission seeks 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 paid for the covered equipment and services or the supplier from whom the equipment was purchased? The Commission also seeks comment on how it could use the information it has already collected to reduce potentially duplicative reporting requirements for carriers.

37. To what extent should the Commission 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, the Commission does not propose to treat as confidential whether a particular provider has covered equipment or services in its network. Moreover, because information on the magnitude of covered equipment and services among individual service providers would be of public interest, the Commission proposes to make such information publicly available. Provider-specific information on the location of covered equipment and services could raise security and confidentiality concerns. Accordingly, the Commission proposes to treat that specific information as presumptively confidential. The Commission seeks comment on these proposals and any alternative proposals.

38. 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. 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 § 1.80 of the Commission's rules. Additional regulations to implement this particular provision appear unnecessary as there are already regulations governing Commission processes regarding forfeiture proceedings. The Commission seeks comment on the assumptions that it needs not propose any new procedural enforcement requirements associated with section 7(a) of the Secure Networks Act.

39. 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." 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." The statute bars violators from further participation in the section 4 reimbursement program, and violators may be barred from participating in other Commission programs, "including the Federal universal service support programs." 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. The Commission proposes to adopt regulations tracking the language contained in section 7

and seek comment on this proposal.

40. 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. The Commission proposes 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?

41. The proposals in the Further Notice generally reflect mandates from the Secure Networks Act, and the Commission has no discretion to ignore such congressional direction. To the extent that the Commission seeks comment on multiple possible options to implement any given mandate, it urges commenters, where possible, to include an assessment of relative costs and benefits for competing options. The proposals in the 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. The Commission further seeks detailed comments on the costs of the proposals in the 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. How can the Commission best incorporate this information into its 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? The Commission seeks comment, generally, on the impact the proposed rules will have on small businesses and steps it can take to mitigate the impact, if any, of these rules on those small businesses.

III. PROCEDURAL MATTERS

A. Paperwork Reduction Act Analysis

42. This document contains proposed new information collection requirements. The

Commission, as part of its continuing effort to reduce paperwork burdens, will invite 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), the Commission seeks specific comment on how it might further reduce the information collection burden for small business concerns with fewer than 25 employees.

43. *Ex Parte Presentations.* This proceeding is a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. 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 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.

44. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), 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

Further Notice. 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 Further Notice provided on the first page of the item. The Commission will send a copy of the Further Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the Further Notice and IRFA (or summaries thereof) will be published in the Federal Register.

45. Consistent with the Commission's obligation to be responsible stewards of the public funds used in the USF programs and increasing concern about ensuring communications supply chain integrity, the Further Notice proposes and seeks comment on rules to implement sections 2, 3, 5, and 7 of the Secure Networks Act and their applicability to the Commission's ongoing efforts to secure the communications supply chain.

46. 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.

47. 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. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act. 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 SBA.

48. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. The Commission's actions, over time, may affect small entities that are not easily categorized at present. The Commission therefore describes in this document, at the outset, three broad groups of small entities that

could be directly affected herein. 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. These types of small businesses represent 99.9% of all businesses in the United States which translates to 28.8 million businesses.

49. 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." 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).

50. 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." U.S. Census Bureau data from the 2017 Census of Governments indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts with enrollment populations of less than 50,000. Accordingly, based on the 2017 U.S. Census of Governments data, the Commission estimates that at least 48,971 entities fall into the category of "small governmental jurisdictions."

51. 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.

52. The Further Notice 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 Further Notice 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. The Commission seeks comment on this proposal, and its likely costs and benefits, as well as on alternative approaches and any other steps it should consider taking.

53. 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."

54. In compliance with the Secure Networks Act, the Further Notice 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 maintain communications equipment and services on the Covered List.

55. The Commission expects to take into account the economic impact on small entities, as identified in comments filed in response to the Further Notice and this IRFA, in reaching our final conclusions and promulgating rules in this proceeding. The Further Notice 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.

IV. ORDERING CLAUSES

56. 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 §§ 1.1 and 1.412 of the Commission's rules, 47 CFR 1.1 and 1.412, the Further Notice IS ADOPTED.

57. IT IS FURTHER ORDERED that the Further Notice will be EFFECTIVE upon publication in the Federal Register, with comment dates indicated therein.

List of Subjects

47 CFR Part 1

Administrative practice and procedure, Civil rights, Claims, Communications, Communications common carriers, Communications equipment, Cuba, Drug abuse, Environmental impact statements, Equal access to justice, Equal employment opportunity, Federal buildings and facilities, Government employees, Historic preservation, Income taxes, Indemnity payments, Individuals with disabilities, Internet, Investigations, Lawyers, Metric system, Penalties, Radio, Reporting and recordkeeping requirements, Security measures, Satellites, Telecommunications, Telephone, Television, Wages

47 CFR Part 54

Communications common carriers, Health facilities, Infants and children, Internet, Libraries, Puerto Rico, Reporting and recordkeeping requirements, Schools, Telecommunications, Telephone, Virgin Islands.

FEDERAL COMMUNICATIONS COMMISSION

Cecilia Sigmund,
Federal Register Liaison Officer.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR parts 1 as follows:

PART 1 – PRACTICE AND PROCEDURE

1. 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 § 1.7004 to subpart V to read as follows:

§ 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 § 1.40002(b) 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 § 1.40002(b) 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 § 1.40002(b) 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 47 CFR 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.

3. Add subpart CC to read as follows:

Subpart CC – Secure and Trusted Communications Networks

Sec.
1.40000 Purpose.
1.40001 Definitions.
1.40002 Covered List.
1.40003 Updates to the Covered List.

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, Public Law 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 § 1.40002.

(e) *External determinations*. The term "external determination" means any determination from sources identified in § 1.40002(b)(1)(i) through (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 § 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 (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 (Pub. L. 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) *External Determination Reversal.* 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 § 1.40002(b)(1)(i) through (iv) maintains an external determination supporting inclusion on the Covered List of such equipment or service.

PART 54 — UNIVERSAL SERVICE

4. 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.

5. Add § 54.10 to subpart A to read as follows:

§ 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 § 1.40001(c) of this chapter.

(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 § 1.40002(b) of this chapter. In the case of any covered communications equipment or service that is on the initial list published pursuant to § 1.40002(b), such equipment or service shall be treated as being placed on the list on the date which such list is published.

6. Add subpart P to read as follows:

Subpart P – Secure and Trusted Communications Networks Reimbursement Program

Sec.

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, Public Law 116-124, 133 Stat. 158.

§ 54.1601 [Reserved]

§ 54.1602 Enforcement.

(a) *General enforcement*. In addition to the penalties provided under the Communications Act of 1934, as amended, and § 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, Public Law 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) of this section 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) of this section.

[FR Doc. 2020-17223 Filed: 8/7/2020 8:45 am; Publication Date: 8/10/2020]