6712-01

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 54

[WC Docket No. 18-89, PS Docket Nos. 19-351, 19-352; FCC 19-121; FRS 16315]

Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) adopts a rule that prospectively prohibits the use of Universal Service Fund (USF or the Fund) funds 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. In doing so, the Report and Order initially designates Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of the rule and establish a process for designating additional covered companies in the future. To support the Commission's future efforts to protect the communications supply chain, the Information Collection Order (Order) directs the Wireline Competition Bureau (WCB) and Office of Economics and Analytics (OEA), in coordination with USAC, to conduct an information collection to determine the extent to which potentially prohibited equipment exists in current networks and the costs associated with removing such equipment and replacing it with equivalent equipment.

DATES: Effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT: For further information, please contact John Visclosky, Competition Policy Division, Wireline Competition Bureau, at John.Visclosky@fcc.gov.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Report and Order and Order in WC Docket No. 18-89 and PS Docket Nos. 19-351 and 19-352, adopted November 22, 2019 and released November 26, 2019. The full text of this document is available for public inspection during

regular business hours in the FCC Reference Information Center, Portals II, 445 12th Street, SW, Room CY-A257, Washington, DC 20554 or at the following internet address: https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf . The Further Notice of Proposed Rulemaking that was adopted concurrently with this Report and Order and Order is published elsewhere in the *Federal Register*.

Comments on the initial designations of Huawei and ZTE as covered companies are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file 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). Interested parties may file comments, identified by PS Docket No. 19-351 for the Huawei final designation proceeding or PS Docket No. 19-352 for the ZTE final designation proceeding, by any of the following methods:

- 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.
    - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

- 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.

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).

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. 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.

I. INTRODUCTION

1. In today's increasingly connected world, safeguarding the security and integrity of America's communications infrastructure has never been more important. Broadband networks have transformed virtually every aspect of the U.S. economy, enabling the voice, data, and Internet connectivity that fuels all other critical industry sectors—including our transportation systems, electrical grid, financial markets, and emergency services. And with the advent of 5G—the next generation of wireless technologies, which is expected to deliver exponential increases in speed, responsiveness, and capacity—the crucial and transformative role of communications networks in our economy and society will only increase. It is therefore vital that the Commission protects these networks from national security threats.

2. The Commission has taken a number of targeted steps to protect the nation's communications networks from potential security threats. In this document, the Commission builds on these efforts, consistent with concurrent Congressional and Executive Branch actions, and ensure that the

public funds used in the Commission's USF funds are not used in a way that undermines or poses a threat to our national security. Specifically, in the Report and Order, the Commission adopts a rule that prospectively prohibits the use of USF funds 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. In doing so, the Commission initially designates Huawei and ZTE as covered companies for purposes of this rule and establish a process for designating additional covered companies in the future.

3. Given the Commission's oversight of the USF programs that fund voice and broadband networks and services and the Commission's obligation to be responsible stewards of the public funds that subsidize those programs, the Commission has a specific, but important, role to play in securing the communications supply chain. The Commission believes that the steps the Commission takes in the document are consistent with this role, that the Commission must do all it can within the confines of its legal authority to address national security threats, and that its actions, along with those taken by other Executive Branch agencies, will go far in securing our nation's critical telecommunications infrastructure.

II. REPORT AND ORDER

4. Based on the Commission's review of the extensive record in the proceeding, it adopts a rule that no universal service support may be used 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. Accordingly, USF recipients may not use USF funds to maintain, improve, modify, operate, manage, or otherwise support such equipment or services in any way, including upgrades to existing equipment and services. This prohibition applies to any subsidiaries and affiliates of USF recipients to the extent that such subsidiaries and affiliates use USF funds.

5. In addition to adopting the rule, the Commission initially designates Huawei and ZTE as covered companies for the purposes of this prohibition. Both companies' ties to the Chinese government and military apparatus—together with Chinese laws obligating them to cooperate with any request by the

Chinese government to use or access their systems—pose a threat to the security of communications networks and the communications supply chain and necessitate taking this step. The Commission's actions in this document are informed by the evidence cited herein, including the actions of other agencies and branches of the government and similar assessments from other countries.

6. As the Commission stated in the *Protecting Against National Security Threats Notice*, the promotion of national security is consistent with the public interest, and USF funds should be used to deploy infrastructure and provide services that do not undermine our national security. The Commission has long accorded significant weight to the views of Executive Branch agencies on matters of national security, foreign policy, law enforcement, and trade policy, and the Commission finds it very significant that the U.S. Department of Justice (DoJ) has expressed its strong support for this conclusion. The Commission also agrees with the Telecommunications Industry Association (TIA) that the Commission "may reasonably conclude that limiting the use of technology from certain vendors deemed to pose a heightened national security risk is an appropriate element of providing a quality communications service." The record persuades the Commission that the nature of today's communications networks is such that untrusted participants in the supply chain pose a serious risk to the integrity and, thus, the quality of those networks.

7. It is well established that the Commission has authority to place reasonable public-interest conditions on the use of USF funds. In the 2011 *USF/ICC Transformation Order*, 76 FR 73830, November 29, 2011, the Commission determined that supported services must be provided using broadband-capable networks and that ETCs must offer broadband services that meet certain basic performance requirements. As the Tenth Circuit held in upholding the Commission's imposition of these obligations, section 254(c)(1) does not limit the Commission's authority to place conditions on the use of USF funds, and section 254(e) is reasonably interpreted as allowing the Commission "to specify what a USF recipient may or must do with the funds," consistent with the policy principles outlined in section 254(b). The Commission adopts the rule as just such a restriction, based on its conclusion that it is critical to the provision of "quality service" that USF funds be spent on secure networks and not be spent

on equipment and services from companies that threaten national security. Or, to put it another way, providing a secure service is part of providing a quality service.

8. The Commission disagrees with commenters who suggest that adopting the rule violates the principle that "[q]uality services should be available at just, reasonable, and affordable rates." As TIA points out, many companies have been able to provide quality services at reasonable and affordable rates using suppliers whose quality, and risk to our national security, is not being questioned here. Furthermore, the Commission is not persuaded by arguments that the proposed rule would violate this principle by eliminating low-cost suppliers. Again, the record clearly demonstrates that service can be provided at just, reasonable, and affordable rates without these suppliers. Additionally, there is evidence that those low costs are likely due to favorable subsidies and other benefits bestowed by governments that are in an adversarial position to the United States. To the extent that certain vendors are able to offer lower prices for their equipment or services due to subsidization from foreign governments that pose a national security threat, restricting federal funding to those vendors should unleash competition from more-trusted, higher-quality suppliers in the long run, resulting in significant public interest benefits. Furthermore, the Commission would be shirking its responsibility to the American public if it were to ignore threats to our security posed by certain equipment manufacturers simply because that equipment was cheaper.

9. Moreover, the Commission must ensure that universal service funds are being spent in a manner consistent with section 254 of the Act. Section 254(e) requires that USF recipients "shall use that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended." This language authorizes the Commission to designate the services for which USF support will be provided and to "encourage the deployment of the types of facilities that will best achieve the principles set forth in section 254(b)." The Commission also must define the services supported by USF, which the statute explains is to be "an evolving level of telecommunications services that the Commission shall establish periodically under this section." In so doing, the Commission "shall consider . . . the extent to which such telecommunications services . . . are consistent with the public interest, convenience,

and necessity." Again, the Commission concludes that the public interest requires that the USF support only services that are not dependent on equipment and services provided or produced by any company that poses a national security threat. The Commission's decision here to limit the services that will be supported by USF is especially consistent with public safety, under section 254(c)(1)(A), and with the public interest, convenience, and necessity, under section 254(c)(1)(D).

10. To the extent parties contend that the Commission may not change what it establishes as the "evolving level of telecommunications services" to be supported by USF without first seeking the recommendation of the Joint Board, the Commission disagrees. Section 254(c)(1) requires the Commission to establish the definition of universal service; it allows the Joint Board to issue a recommendation but does not require Commission action to be preceded by such a recommendation. The Commission has acted under this provision several times without following a recommendation of the Joint Board—for example in the *2014 First E-Rate Order*, 80 FR 167, January 5, 2015, and the *2016 Lifeline Order*, 81 FR 33026, May 24, 2016.

11. The Commission also rejects arguments that it may not consider national security in assessing the public interest generally or under section 254. Indeed, the security of our nation is an important part of the public interest. That's why the Commission has consistently held, including in the *Protecting Against National Security Threats Notice* in the proceeding, that national security concerns are part of the public interest and that the Commission's exercise of specific statutory authorities should, when warranted, take those concerns into account. As discussed in the *Protecting Against National Security Threats Notice*, the Commission adopted rules implementing the 2012 Spectrum Act to prohibit participation in spectrum auctions by entities that have been barred by any federal agency from bidding on a contract, participating in an auction, or receiving a grant. The Commission also has a long history of considering national security equities where other agencies have specific expertise and are positioned to make recommendations, and adopting a similar process here cannot be characterized as "promot[ing] other, unrelated objectives" unrelated to the specific regulatory program at hand.

12. More generally, section 201(b) of the Act authorizes the Commission to promulgate

"such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act." It is well-established that the promotion of national security is consistent with the public interest and part of the purpose for which the Commission was created. As section 1 of the Act states, the Commission was created "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 . . . ." The Commission concludes based on the record of the proceeding that it is necessary in the public interest to prohibit USF recipients from spending universal service funds on covered equipment or services.

13. The action the Commission takes in this document also implements section 105 of the Communications Assistance for Law Enforcement Act (CALEA). That section requires every telecommunications carrier to ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only pursuant to a lawful authorization and with the affirmative intervention of an officer or employee of the carrier. The Commission has concluded that all facilities-based providers of broadband Internet access services and all providers of interconnected VoIP services are telecommunications carriers under CALEA. The Commission has interpreted "switching premises" consistent with the purpose of CALEA as including "routers, soft switches, and other equipment that may provide addressing and intelligence functions for packet-based communications to manage and direct the communications along to their intended destinations." One of the dangers of allowing equipment from untrusted suppliers to be part of a network is the possibility that those suppliers will maintain the ability to illegally activate interceptions or other forms of surveillance within the carrier's switching premises without its knowledge, whether through the insertion of malicious hardware or software implants, remote network access maintained by providers of managed services, or otherwise. Telecommunications carriers, including all ETCs, therefore appear to have a duty to avoid such risks.

14. The Commission disagrees with Huawei that its recognition of this duty is barred by section 103(b)(1) of CALEA, 47 U.S.C. 1002(b)(1). The rule the Commission adopts in this document addresses only the use of USF funds and does not prohibit the "adoption of any equipment."

Furthermore, the Commission is not a "law enforcement agency" within the meaning of section 103(b)(1); in the context of CALEA, that term refers to agencies that conduct interceptions and access to call-identifying information.

15. The Commission is authorized to "prescribe such rules as are necessary to implement the requirements of" CALEA and specifically to require carriers to establish policies and procedures to prevent unauthorized surveillance. Though the rule the Commission adopts in this document applies only to ETCs' use of USF funds, it disagrees with Huawei's argument that the link between this obligation and the prohibition the Commission adopts here is "remote." The rule the Commission adopts in this document directly implements section 105 of CALEA by reducing the likelihood that ETCs use USF funds to facilitate unauthorized surveillance. Nor does the rule require, as Huawei suggests, that the Commission interprets section 105 "as prohibiting carriers from using any equipment that has *any* possibility, no matter how remote, of being subject to unauthorized access for purposes of intercepting communications." But use of equipment or services from companies that pose national security threats is far more likely to be subject to such unauthorized access, and the Commission chooses here not to allow USF funds to support such use.

16. The Commission further disagrees with Huawei's contention that CALEA's security provision does not apply to attempts by actors other than U.S. law enforcement to intercept or access communications. The plain language of section 105 specifies not only the activation of the assistance capabilities required by section 103 but any interception or access effected within a carrier's switching premises. This understanding of the plain language is consistent with its legislative history. The bills reported by the House and Senate Judiciary Committees used different language limiting the security obligation only to "any court ordered or lawfully authorized interception of communications or access to call-identifying information within its switching premises," but that language was revised in consultation with the House Energy and Commerce Committee in the version of the bill ultimately considered and adopted on the floor of both Houses. The Commission considers the change to be purposeful and to reflect Congress's understanding of CALEA as enacting protections against unauthorized surveillance,

not only as ensuring the ability of law enforcement to conduct authorized surveillance.

17. Congress has also determined, in section 889 of the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA), that the expenditure of loan or grant funds by federal agencies to procure or obtain covered telecommunications equipment or services is contrary to the security interests of the United States. Although the USF is neither a loan program nor a grant program, it is a significant source of funds administered by the Commission and intended for the purchase of equipment, services, or systems with which section 889 is concerned. The Commission finds that the goals underlying section 889 of the 2019 NDAA also support its decision to take action here. Following enactment of the 2019 NDAA, the WCB sought comment on the relevance of section 889(b)(1) to the proceeding. The record now persuades the Commission that adoption of a rule that prohibits universal service funds from being used to obtain equipment or services produced or provided by companies that pose a threat to national security, and the Commission's initial designation of Huawei and ZTE as such companies, is consistent with section 889 of the 2019 NDAA. The Commission agrees with TIA that section 889 "codifies a determination by Congress regarding five specific suppliers of concern," including Huawei and ZTE, and expresses a view that "the role of the Commission and other executive agencies is to prevent the use of federal funds under their control on equipment and services from [those] suppliers of concern."

18. The Commission establishes a process for designating entities as national security threats for purposes of its rule. The Commission first defines "covered company" to include subsidiaries, parents and affiliates of covered companies for purposes of the rule it adopts in this document. In the *Protecting Against National Security Threats Notice*, the Commission sought comment on whether a covered company's subsidiaries, parents, and/or affiliates should be treated as a covered company as well and sought comment on how to define such entities. Because equipment from subsidiaries, parents, and affiliates pose the same risks to network integrity as equipment directly from the covered company, the Commission includes any subsidiary, parent, or affiliate of a covered company as a covered company subject to its prohibition.

19. When the Commission initially determines, either *sua sponte* or in response to a petition

from an outside party, that a company poses a national security threat to the integrity of communications networks or the communications supply chain, the Commission will issue a public notice advising that such initial designation has been made, as well as the basis for such designation. This public notice shall serve as an "initial designation" of a covered company. Upon the issuance of such notice, interested parties may file comments responding to the initial designation, including proffering an opposition to the initial designation. If the initial designation is unopposed, the entity shall be deemed to pose a national security threat 31 days after the issuance of the notice. If any party opposes the initial designation, the designation shall take effect only if the Commission determines that the affected entity should nevertheless be designated as a covered company under the Commission's rule. In either case, the Commission shall issue a second public notice announcing its final designation and the effective date of that final designation. This public notice shall serve as the "final designation" of a covered company. In order to provide regulatory certainty to entities affected by initial designations, the Commission shall make a final designation effective no later than 120 days after release of its initial designation notice. The Commission may, however, extend such 120-day deadline for good cause.

20. In formulating its initial and final designations, the Commission will use all available evidence to determine whether an entity poses a national security threat. Examples of such evidence may include, but are not limited to: determinations by the Commission, Congress or the President that an entity poses a national security threat; determinations by other executive agencies that an entity poses a national security threat; and, any other available evidence, whether open source or classified, that an entity poses a national security threat. Where appropriate, the Commission will seek to harmonize its determinations with the determinations of other federal agencies in the Executive branch and determinations of the Legislative branch. The Commission will base its determination on the totality of evidence surrounding the affected entity and should consider any evidence provided by the affected entity, or any other interested party, in making its final determination. However, classified information will not be made public, nor will it be made available to the designated company.

21. *Reversal of Designation.* The Commission will act to reverse its designation upon a

finding that a covered company no longer poses a national security threat to the integrity of communications networks or the communications supply chain. A covered company, or any other interested party, may submit a petition asking the Commission to remove a designation based on a showing of changed circumstances. The Commission shall seek the input of Executive Branch agencies and the public upon receipt of such a petition. If the record shows that a covered company is no longer a national security threat, the Commission shall promptly issue an order reversing its designation of that company. The Commission may dismiss repetitive or frivolous petitions for reversal of a designation without notice and comment—and may dismiss petitions that make no showing of changed circumstances or attempt to evade the limits the Commission's rules place on petitions for reconsideration or applications for review. If the Commission reverses its designation, it shall issue an order announcing its decision along with the basis for its decision.

22. In the *Protecting Against National Security Threats Notice*, the Commission highlighted the longstanding concerns about the threats posed by Huawei and ZTE, including by other Executive Branch agencies and Congress. Both companies, as well as their subsidiaries and affiliates, are restricted from selling certain equipment and services to federal agencies due to Congressional and Executive Branch concern about the threat their equipment and services pose to the communications supply chain. Huawei vigorously responded to these allegations in the record of the proceeding, and ZTE did not make any filings in the proceeding. The Commission's examination of the record re-affirms the concerns raised by them in the *Protecting Against National Security Threats Notice*, and the Commission therefore takes the step of initially designating Huawei and ZTE as covered companies for purposes of the prohibition the Commission adopts in this document.

23. The Commission concludes that publicly available information in the record is sufficient to support these designations. In addition, the Commission has compiled and reviewed additional classified national security information that provides further support for its determinations.

24. The Commission agrees with commenters who argue that "state actors, most notably China and Russia, have supported extensive and damaging cyberespionage efforts in the United States,"

and there exists a "substantial body of evidence" about the risks of certain equipment providers like Huawei and ZTE. International experts have found that China has a "notorious reputation for persistent industrial espionage, and in particular for the close collaboration between government and Chinese industry." Allies of the United States have discovered numerous instances where the Chinese government has engaged in malicious acts, including "actors likely associated with the . . . Ministry of State Security . . . responsible for the compromise of several Managed Service Providers." And as noted in the *2012 HPSCI Report*, Huawei and ZTE are the "two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States."

25. These two companies pose a great security risk because Chinese intelligence agencies have opportunities to tamper with their products in both the design and manufacturing processes. The *2012 HPSCI Report* observed that the risks posed by companies such as Huawei are further exacerbated because the company offers services managing telecommunications equipment and its "authorized access" could be exploited "for malicious activity under the guise of legitimate assistance." This legislative concern has continued, with Congress passing, and the President signing into law, significant restrictions on the purchase of equipment and services from Huawei and ZTE. And, in the proceeding, the Attorney General has agreed that "a company's ties to a foreign government and willingness to take direction from it bear on its reliability" for building or servicing telecommunications networks with the support of federal funds. As explained in the following, the Commission believes that Huawei and ZTE pose a unique threat to the security of communications networks and the communications supply chain because of their size, their close ties to the Chinese government both as a function of Chinese law and as a matter of fact, the security flaws in their equipment, and the unique end-to-end nature of Huawei's service agreements that allow it key access to exploit for malicious purposes. As a consequence, the Commission's primary focus is on Huawei and ZTE.

26. The Commission notes, at the outset, that the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any

governmental requests, which could involve revealing customer information, including network traffic information. The Department of Justice says that the Chinese government "has subsidized [its] firms to lock up as much of the market as possible," which "threatens to thwart the emergence of fair competition and lead to irreversible market dominance that will force all of us onto Chinese systems, causing unmitigable harm to our national security." According to Article 7 of the Chinese National Intelligence Law (NIL), all "organizations and citizens shall, according to the law, provide support and assistance to and cooperate with the State intelligence work, and keep secret the State intelligence work that they know." Article 14 permits Chinese intelligence institutions to request that Chinese citizens and organizations provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment. The Chinese NIL is extremely broad, applying to Chinese citizens residing outside of China. Article 11 specifies that the law's powers are not limited to Chinese soil, which would permit Chinese government elements to compel Huawei and ZTE to carry out their directives within the United States' national boundaries. Further, Article 28 of the NIL allows personnel to be punished for violating the Chinese NIL. This broad authority to compel support and assistance to Chinese intelligence agencies is particularly troublesome, given the Chinese government's involvement in computer intrusions and attacks as well as economic espionage. As a consequence, the Commission's primary focus in the Report and Order is on Huawei and ZTE.

27. The Commission initially designates Huawei, along with its parents, affiliates, and subsidiaries, as a covered company for purposes of the Commission's rule.

28. The Commission finds that Huawei's ties to the Chinese government and military apparatus, along with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their system, pose a threat to the security of communications networks and the communications supply chain. Congress and the Executive Branch have repeatedly expressed concerns regarding Huawei, its ties to the Chinese government, and its equipment. In addition to reports recommending that government agencies, federal contractors, and private-sector entities consider

excluding Huawei and ZTE equipment from their networks due to long-term security risks and the companies' close ties to the Chinese government, Congress has also taken action to limit the purchase of certain Huawei and ZTE equipment and services for federally funded networks. Additionally, the Department of Commerce has added Huawei to its Entity List, which "identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States." These concerns center around Huawei's established relationship with the Chinese government as well as Huawei's obligation under Chinese law to cooperate with requests by the Chinese government for access to their system.

29. Although Huawei argues that its affiliates in the United States are not subject to state security laws, the Commission is not persuaded to excuse these affiliates from the scope of the Commission's prohibition. One expert has noted that the nature of the Chinese system "recognizes no limits to government power." Irrespective of their physical location, these affiliates still remain subject to Chinese law.

30. As the House Permanent Select Committee on Intelligence found, "the Chinese government and the Chinese Communist Party . . . can exert influence over the corporate boards and management of private sector companies, either formally through personnel choices, or in more subtle ways." For example, Huawei's founder, Ren Zhengfei, is himself believed to be a former director of the People's Liberation Army Information Engineering Academy, an organization associated with China's signals intelligence. Ren Zhengfei exercises "ultimate veto authority over the company's material decisions." Additionally, the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions. The House Permanent Select Committee on Intelligence also received internal Huawei documentation from former Huawei employees "showing that Huawei provides special network services to an entity the employee believes to be an elite cyber-warfare unit within the PLA."

31. Moreover, analysts have found that while "Huawei claims the Chinese state has no

influence over its activities, . . . the company is treated as a state-owned enterprise and has benefited from state procurement funds, subsidized financing from state-owned policy banks and state funding for research." Huawei is reported to benefit from vast subsidies from the Chinese government, to include state-controlled financial organizations. One study "identified 32 cases since 2012 where Huawei projects were funded by Exim Bank of China ($2.8 billion) or China Development Bank ($7 billion)." In 1998, it was reported that China Construction Bank provided over $470 million in lines of credit to foreign companies as incentive to purchase Huawei products. This initiative accounted for over 45% of the bank's annual extension of credit. While Huawei has refused to answer questions about its ownership and governance, it can be inferred that the Chinese government clearly has a vested interest in the company's success.

32. The Commission's actions in this document are also informed by the actions of other agencies and branches of the government, along with the increasing caution urged by our nation's intelligence officials. For example, in February 2018, the leaders of all six top U.S. intelligence agencies warned against purchasing products or services from Huawei or ZTE with FBI Director Chris Wray saying, "the Commission is deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share the Commission's values to gain positions of power inside our telecommunications networks that provides the capacity to exert pressure or control over the Commission's telecommunications infrastructure." The Department of Justice (DoJ) has also stated its "strong[] support" for the Commission's action in this document, noting that it is pursuing numerous criminal charges against Huawei for violations of federal law and "a willingness to break U.S. law combined with a determination to avoid the consequences by obstructing justice argues against the reliability of the provider."

33. In initially designating Huawei as a covered company, the Commission also relies on similar assessments by other countries. For example, on October 9, 2019, the European Union, with the support of the European Commission and the European Union Agency for Cybersecurity, released its risk assessment on 5G Security, specifically finding a high security risk where hostile countries exercise

pressure on suppliers to facilitate cyberattacks serving their national interests. Many of our allies, including Australia, New Zealand, and Japan, have taken steps to exclude Huawei equipment from their networks. While Huawei argues that its equipment is used in other countries without undermining any nation's security, several of the United States' closest allies have concluded that the risk posed by Huawei equipment and systems is too great to bear. In November 2018, New Zealand's intelligence agency barred its largest telecommunications carrier, Sparc, from using Huawei equipment. Likewise, in December 2018, Japan excluded Huawei from its domestic communications infrastructure. Additionally, in August 2019, the Australian government announced a ban on Huawei equipment. The Commission also notes that communications service providers in other countries, including BT, Orange, and Deutsche Telekom, are acting to keep Huawei equipment out of their 5G networks.

34. Moreover, the Commission is confident that the national security risk to our communications network from permitting Huawei equipment and services is significant. For example, in 2019, Finite State, a cybersecurity firm, issued a report describing the unique threat posed by Huawei's "high number" of security vulnerabilities. The report found that over half of the Huawei firmware images analyzed had at least one potential backdoor that could allow an attacker with knowledge of the firmware to log into the device, and that Huawei continues to make firmware updates without addressing these vulnerabilities. Finite State articulates the concern that suppliers of technology, such as Huawei, with "secret or overt access to the infrastructure they are providing," could use that access "in times of peace, or perhaps [for] something far more ominous in times of conflict."

35. Also in 2019, the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board released a report that sounded the alarm about the risks associated with Huawei's engineering processes. The report further revealed that Huawei had made no substantive gains in the remediation of issues reported in the previous year, noting that, "[a]t present, the Oversight Board has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation program that it has proposed as a means of addressing these underlying defects." Further, in a 2013 report, the Intelligence and Security Committee of the UK Parliament said, "theoretically, the

Chinese State may be able to exploit any vulnerability in Huawei's equipment in order to gain some access to the BT network, which would provide them with an attractive espionage opportunity."

36. Furthermore, a recent report from Recorded Future, a cyber threat intelligence firm, found that "[t]he enormous range of products and services offered by Huawei generates a nearly unimaginable amount of data for one company to possess." This problem is compounded by Huawei's "desire to be an end-to-end provider for whole network solutions." As the *2012 HPSCI Report* found, when companies "seek to control the market for sensitive equipment and infrastructure that could be used for spying and other malicious purposes, the lack of market diversity becomes a national concern for the United States and other countries." Huawei's desire to limit diversity in equipment poses a threat to the security of U.S. communications networks. Its access to this vast amount of data combined with its close ties to the Chinese government and its obligation under Chinese law to assist with Chinese intelligence-gathering mean that "Huawei is potentially subjected to a government-driven obligation to capitalize on its global network and consumer devices ecosystem to fulfill core [Chinese government] national security and economic dominance objectives." Given the multitude of evidence about the threat that Huawei equipment presents, along with the company's unique and close relationship to the Chinese government, the Commission disagrees with Huawei's claim that there is no support for the conclusion that its equipment poses a threat. The fact that Huawei's subsidiaries act outside of China does not mean that their parent company lacks influence over their operations and decisions given the strong influence that Huawei's parent companies and the Chinese government can exert over their affiliates. The Commission additionally disagrees with Huawei's assertion that the Chinese NIL is irrelevant because it is merely a "defensive measure" that does not "provide authority for Chinese intelligence agencies to engage in offensive intelligence activities." The broad nature of the Chinese NIL, along with the Chinese government's control over Huawei and history of espionage activities, presents far too great a risk to the security of U.S. communications networks to rely on the assurance that the Chinese government will act only in a vaguely-defined "defensive" manner. While the Commission recognizes that the Chinese NIL may be interpreted in different ways, the fact remains that entities such as Huawei that are subject to the

NIL, and subject to the Chinese legal regime generally, pose too great a risk to the security of communications networks and the communications supply chain.

37. The Commission also disagrees with Huawei's criticisms of the Finite State report. Huawei argues that the Finite State report focused on old versions of Huawei's equipment and did not follow "general practices" of security testing, which it argues, "typically involves dialogue between the security company and vendor" about vulnerabilities. However, unlike a report that assesses a zero-day threat and would typically include dialogue with the vendor to provide time to mitigate the threat, Finite State's report was a general risk analysis report and was focused primarily on the culture of risk management at Huawei. In response to Huawei's public criticisms of its report, Finite State determined that, "Based on 8 years of analysis of [UK Huawei Cyber Security Evaluation Centre] reports, along with the recent Finite States analysis, the Commission can clearly see that Huawei's security posture has not materially improved over time." Indeed, the Commission agrees with Finite State that "Huawei cannot deny that, now, multiple organizations have independently found similar, substantial security vulnerabilities in their products."

38. In the light of the record in the proceeding and other publicly available information detailing the scope of the risk of allowing Huawei's equipment and services into our communications networks, and given that the Chinese government has the "means, opportunity, and motive to use telecommunications companies for malicious purposes," the Commission concludes that Huawei, its parents, affiliates, and subsidiaries should be initially designated as a national security threat to the integrity of communications networks or the communications supply chain for purposes of the rule the Commission adopts in this document.

39. The Commission also initially designates ZTE, its parents, affiliates, and subsidiaries as a covered company for purposes of the Commission's rule.

40. As with Huawei, ZTE has close ties to the Chinese military apparatus, having originated from the Ministry of Aerospace, a government agency. In fact, ZTE is still alleged to be partially owned by the Chinese government. As the House Permanent Select Committee on Intelligence found, ZTE is in

essence, "a hybrid serving both commercial and military needs." In particular, much of ZTE's ownership constitutes state owned enterprises, and, like Huawei, ZTE contains an internal Communist Party Committee, as required by the laws of China. The House Permanent Select Committee on Intelligence also found that ZTE has not allayed the Committee's concerns that it "is aligned with Chinese military and intelligence activities or research institutes." As described in this document, legislative concern with ZTE equipment and services has been ongoing, with Congress passing, and the President signing into law, significant restrictions on the purchase and use of ZTE equipment.

41. Open source information highlights the risks posed by ZTE equipment. In April 2018, the Department of Defense announced that ZTE and Huawei devices would no longer be offered for sale at U.S. military bases and ordered them removed from its stores worldwide. In August 2018, a report funded by the Department of Homeland Security's Science and Technology Directorate found a wide range of vulnerabilities in a number of mobile devices manufactured and marketed by ZTE. The report indicated that the vulnerabilities are built into the phones during the manufacturing process and could allow malicious access to user data. While the USF generally does not fund end-user devices such as phones, the security concerns raised regarding ZTE mobile phones give the Commission concerns about other ZTE equipment and services, including those funded by the USF. The National Security Institute published a report in January 2019 that describes the underlying risks posed by both Huawei and ZTE systems and recommends "additional restrictions on Huawei and ZTE products and services in the U.S." As with Huawei, ZTE's equipment has been barred in Australia and New Zealand.

42. Finally, the DoJ, in supporting the Commission's initial designations of Huawei and ZTE, has noted that ZTE pleaded guilty to violating our embargo on Iran by sending approximately $32 million dollars' worth of U.S. goods to Iran and obstructing justice in an effort to thwart DoJ's investigation. Such disregard for American law in furtherance of the interests of foreign governments is additional evidence of the danger posed by Huawei and ZTE equipment in our communications networks.

43. Given that the Chinese government has the "means, opportunity, and motive to use telecommunications companies for malicious purposes," the Commission concludes that ZTE

Corporation, its parents, affiliates, and subsidiaries should be initially designated as a national security threat to the integrity of communications networks or the communications supply chain for purposes of the rule the Commission adopts in this document.

44. The Commission directs the Public Safety and Homeland Security Bureau (PSHSB) to implement the next steps in the designation processes for Huawei and ZTE. The Commission also directs PSHSB going forward to make both initial and final designations, to reverse prior designations, and to issue the public notices required in the designation process. PSHSB shall have discretion to revise this process if appropriate to the circumstances, consistent with providing affected parties an opportunity to respond and with any need to act expeditiously in individual cases. To the extent that a designated entity seeks review of a designation decision—from either PSHSB or the full Commission—PSHSB or the Commission shall act on such petition for reconsideration or application for review, respectively, within 120 days of the filing by a designated entity. The Commission finds that this time limitation is important to provide regulatory certainty to entities affected by designations made at the Commission or bureau level, and consistent with the national security interests at stake. The Commission or PSHSB may, however, extend such 120-day deadline for good cause.

45. *Huawei and ZTE*. The designations adopted herein for Huawei and ZTE shall serve as initial designations. Interested parties may file comments responding to these initial designations. Such comments are due 30 days after publication of the Report and Order in the *Federal Register*. After the conclusion of the comment period, PSHSB shall issue a public notice announcing its final determination and the effective date of any final designation.

46. The Commission next establishes the scope of the new prohibition. The rule the Commission adopts in the Report and Order shall apply to any and all equipment or services, including software, produced or provided by a covered company. USF recipients must be able to affirmatively demonstrate that they have not used any funds obtained via the USF to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by a covered company.

47. The Commission finds it necessary to establish this broad prohibition on the use of USF funds to procure or otherwise support any and all equipment and services produced or provided by a covered company. Although some commenters argue that a prohibition precluding the expenditure of USF funds on *every* product from a covered company would not advance any material security purpose, and that such a restriction would be overbroad with potentially negative repercussions for U.S. industry, both domestically and overseas, the Commission believes that a blanket prohibition best promotes national security, provides the most administrable rule, and eases compliance for USF recipients. Given the dynamic and wide-ranging nature of the potential threats to our networks, and the Commission's specific responsibility to protect against threats posed by USF-funded equipment and services, the Commission finds a complete prohibition on the expenditure of USF funds on any and all equipment and services from a covered company to be the only reliable protection against potential incursions. The Commission recognizes that a complete prohibition may impose attendant costs on providers, who must ensure that equipment or services obtained using USF funds do not use equipment or services produced or provided by a covered company, and the rural consumers served by these providers. However, the Commission finds that these costs are outweighed by the need to ensure that the services funded by USF are secure and by the benefits to our national security and the nation's communications networks.

48. Malware and vulnerabilities can be designed and built directly into communications equipment, even when that equipment is not the covered company's flagship equipment. Thus, these vulnerabilities can often be difficult to discover. Moreover, the transition to emerging next-generation networks and the accelerated adoption of virtualized distributed network infrastructure increases the number of attack points in the network and makes networks more susceptible to attacks and unauthorized intrusions. Given the increased risk that allowing any equipment from a covered company on the network can cause significant harm, the Commission cannot allow for bad actors to circumvent the Commission's prohibitions through clever engineering.

49. The Commission further finds that a complete prohibition on the expenditure of USF funds for all equipment and services produced or provided by a covered company will provide regulatory

certainty and will be easier for providers to implement and for the Commission to enforce. The Commission agrees with Vermont Telephone, which argues that the Commission's rule "would eliminate uncertainty and reduce regulatory burdens that fall most heavily on small operators," and that adopting the Commission's rule would "level the competitive playing field by creating incentives for operators to secure their networks rather than opting to deploy lower-cost Chinese manufactured equipment." The Commission's decision to adopt a complete prohibition rather than a narrow one will greatly reduce administrative costs for both providers and consumers as it would be time consuming and costly to require determinations on a product-by-product basis as to whether any given equipment is subject to the prohibition. Relatedly, it will be simpler for participants, and thus more cost effective, to comply with a blanket ban on the use of USF funds on any and all equipment and services produced or provided by covered entities. Compliance costs will also be reduced because providers will more easily be able to certify that their subsidiaries and affiliates have not used USF funds to purchase, obtain, maintain, improve, modify, or otherwise support any equipment of a covered company. It would be far more difficult, costly, and invasive for the Commission to obligate providers to verify this same commitment on a product-by-product or even component-by-component basis. By the same token, it will be far simpler and more cost-effective for Universal Service Administrative Company (USAC) to audit and verify any such certification based on a blanket ban rather than a more selective product-by-product prohibition.

50. The Commission is not persuaded that uncertainty in the purchasing process dictates a narrower prohibition. Some commenters argue that it is difficult to know from which companies they are purchasing equipment and that a blanket prohibition within the USF is therefore unreasonable. They claim this difficulty is especially apparent in instances of "white labeling," where a covered company provides equipment or services to a third-party entity for sale under that third party's brand and the purchaser may not know the covered company's equipment is part of the purchased product. Although the Commission understands the complications inherent in the purchasing process, it believes it is the responsibility of all USF recipients to work with their suppliers to understand what equipment and

services they are purchasing and to ensure that such equipment and services are not produced or provided by a covered company. Indeed, were the Commission to find white labeling as outside the scope of its prohibition, it would create an obvious and transparent loophole for companies that pose a national to national security to sneak their equipment into our communications networks.

51. The Commission also makes clear that USF recipients may continue to use these federal funds to maintain, improve, modify, or otherwise support their communications networks generally so long as no such funding goes toward any equipment or services provided or manufactured by a covered company. For example, a USF recipient could use funding to maintain gas-powered generators or battery cells that provide back-up power to radio access network equipment, purchase backhaul facilities and interconnection services from third parties, upgrade and maintain switches and routers, and otherwise expend USF funds on equipment and services that support a provider's network in whole or in part and are not solely used in the maintenance or support of covered equipment. In contrast, a USF recipient could not use federal funds to upgrade covered equipment, install software updates on such equipment, or pay for a maintenance contract to the extent that contract covers covered equipment—even when such upgrades, installations, and contracts are not directly offered by a covered company. Similarly, a USF recipient would not be permitted to use USF support to pay its internal staff to perform maintenance on any equipment or services produced or provided by a covered company. Such expenditures would be directly and solely targeted at supporting equipment that poses a national security threat to our communications networks and allowing such expenditures to be paid for with federal funds would counter the Commission's goal of securing American communications networks and incentivizing the replacement of such equipment with equipment from trusted vendors.

52. The Commission notes that its rule does not prohibit USF recipients from using their own funds to purchase or obtain equipment or services from covered companies, but USF recipients must be able to clearly demonstrate that no USF funds were used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by a covered entity. But the Commission cautions USF recipients that choose to install new equipment or purchase new services from

covered companies. Where a project involves the purchase of such equipment, the Commission believes it unlikely that many USF recipients will be able to show the detailed records necessary to demonstrate that no USF funds were used on equipment or services from a covered company on any part of that project. For example, if a USF recipient tried to install a new cellular radio base station from a company that has been designated as a national security threat, all labor and other expenditures for that installation are part and parcel of installing an insecure network. The Commission is thus skeptical that any USF recipient seeking to use USF funds on an "eligible" portion of such a project would will be able to establish with the necessary certainty, even with a detailed recordkeeping process in place, that no part of the installation process, including the base station and any and all related expenditures, are paid for using USF funds. However, the Commission does not entirely foreclose the possibility that a USF recipient might be able to segregate the use of federal funds from other funds for the completion of a particular project, and the Commission reminds recipients that such expenditures will be subject to the audit and enforcement mechanisms described herein.

53. The Commission agrees with commenters who suggest a whole-of-government approach to supply chain security. The Commission's oversight of the USF requires them to act so that USF funds are not used in a manner that undermines the security of communications networks. In addition, the Commission has a responsibility to act in order to support the ongoing efforts of the federal government to protect communications networks and the communications supply chain from security threats. The prohibition the Commission adopts in this document applies only to equipment and services in the context of the USF, so the Commission believes this limited application of the prohibition will advance the interests of network security and will provide necessary certainty to affected USF participants. In short, the Commission's actions in the Report and Order *are* a vital part of that approach and will complement the activities of other federal agencies and Congress.

54. The Commission disagrees with RWA, which contends that the prohibition it adopts in this document should extend only to "additional equipment" and "new services" not yet procured and deployed; such a distinction would do nothing to address the threat posed by existing equipment. If

anything, it would magnify this risk by enabling providers to continue to use USF support to maintain, improve, modify, operate, manage, renew, or otherwise support such equipment. Restricting the prohibition the Commission adopts in this document to apply only to equipment that has not yet been purchased would not only undercut the purpose behind this proscription, but could actively increase the risks posed by existing equipment.

55. The Commission acknowledges the concerns of some commenters who contend that "rural co-ops and closely held companies are massively restricted in their financial operations" and argue that USF support is "often critical" in order to maintain the operational viability of their networks. While this may be true in the case of some rural carriers, the Commission is unwilling to allow USF dollars to be used in support of equipment and services that pose a direct and immediate threat to our national security and the security of our networks. To do so would place our communications networks and supply chains as a whole at risk. No provider has yet offered the detailed financial records that would be necessary for the Commission to determine whether an individual provider actually could not maintain its existing network without violating its rule—and the Commission reminds providers that they remain free to seek a waiver of this prohibition in the exceptional case where they would be unable to operate their networks absent the use of USF funds to maintain or otherwise support equipment or services produced or provided by covered companies.

56. While the rule the Commission adopts in this document will not, in and of itself, completely address the risks posed by equipment or services produced or provided by covered companies, that is no reason not to adopt the rule, as RWA appears to argue. As the Commission has already stated, the targeted rule it adopts in this document is part of the Commission's continuing efforts to protect the nation's communications networks and supply chain from potential security threats. These efforts are, by their very nature, ongoing and incremental. The Commission's is a specific but nevertheless important role in securing the communications supply chain and our nation's communications infrastructure.

57. *Upgrades to Existing Equipment*. The Commission next clarifies that the prohibition will apply to upgrades and maintenance of existing equipment and services. As explained in this document,

this restriction includes a prohibition on using USF funds to pay third parties or a carrier's own employees to maintain or repair equipment from covered services. Costs for such services must be paid with non-USF funds. The rule the Commission adopts in this document prohibits USF recipients from using USF funds to purchase, obtain, maintain, improve, modify, or otherwise support equipment or services provided or produced by covered companies in addition to purchasing such equipment or services. The Commission specifically extends this prohibition to include upgrades to existing equipment and services. Several commenters have argued that upgrades to existing equipment should be exempt from the Commission's rule, claiming any prohibition on the use of USF funds to support upgrades to existing equipment would "effectively mandate replacement of those products before the end of their life-cycle or force companies receiving USF monies to run outdated or inadequately maintained equipment." Others argue that such upgrades should be exempted because they are necessary to preserve equipment functionality, performance, and security.

58. The Commission recognizes that this rule may encourage some providers to choose not to upgrade equipment and instead to replace these products prior to the end of their life-cycle, or risk running outdated and inadequately maintained equipment. The Commission notes that such upgrades are in fact in the public interest because they would increase the security of our communications networks. Indeed, the Commission finds the risk posed by covered companies' products is too great to continue to allow federal funds to be used to purchase, obtain, maintain, improve, modify, or otherwise support them. To do so would allow these funds to be used to perpetuate existing security risks to the communications supply chain and the communications networks of this country. Further, the Commission is not restricting USF recipients from performing needed upgrades or maintenance to equipment procured from a covered company so long as they do not use USF funds to do so. Although the Commission may have concerns, it acknowledges that providers may continue to use and improve such equipment consistent with all other legal requirements, but they may not perform such maintenance or upgrades using USF funds. Affected carriers may of course file a request for waiver if they are manifestly unable to maintain their networks absent the use of USF funds to support equipment or services produced or provided by

covered companies, and such failure poses a risk to public safety. The Commission evaluates waivers on a fact-specific basis.

59. *Compliance Certifications*. The Commission agrees with commenters who argue that the Commission should require recipients of universal service support to provide a certification that they have complied with the rule it adopts in this document. The Commission does not, at this time, require manufacturers to submit separate certifications, although USF recipients may require such certifications from manufacturers as part of their own contracts. The Commission directs WCB, in coordination with USAC, to revise the relevant information collections for each of the four USF programs to require a certification attesting to compliance with the rule adopted in this document. Given the variety of ways that USF participants file and certify to rule compliance, the Commission finds that directing WCB to develop such a certification for each respective program is the best means by which to implement this new certification requirement.

60. *Audits and Recovery of Funds*. The Commission believes that USAC audits are the most effective way to determine compliance with the requirements of the Report and Order, and the Commission directs USAC to implement audit procedures for each program consistent with the rules it adopts in this document. USF recipients must be able to affirmatively demonstrate that no universal service funds were used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by covered companies. The Commission notes that applicants in the E-rate and Rural Health Care programs already retain and provide information either during the application process or during audit and program integrity assurance processes that could demonstrate (if verified) that no USF funds were improperly used. And the Commission notes that many ETCs receiving High Cost funding now report the projects they complete using federal funds to the High Cost Universal Broadband portal, allowing relatively swift verification by USAC of compliance. If USAC knows the specific locations where federal funds were used to build communications networks, it can verify what equipment and services are used at those locations and audit that usage if necessary. To the extent that other ETCs do not yet report information to USAC that would verify compliance, the

Commission directs WCB and USAC to revise its information collection and audit procedures to ensure the reporting of USF expenditures in a manner that will allow efficient oversight and thorough compliance.

61. Some commenters have argued that, for purposes of the E-Rate and Rural Health Care programs, service providers are in the best position to prevent violations of the rule and, as a result, should be the party responsible for recovery in cases where funds have been disbursed in violation of the rule. The Commission sees no reason to depart from the requirement that directs USAC to pursue recovery actions against the party or parties that committed the rule or statutory violation in question, recognizing that, in some instances, this could be the applicant school, library, health care provider, or consortium, rather than the service provider. The determination of which entity to seek recovery from is a factual determination based on the specific facts of the violation, and the Commission sees no need to establish a rule requiring recovery only from service providers.

62. *Waivers*. The Commission agrees with commenters who support a meaningful waiver process. As with any Commission rule, USF recipients may seek waivers of the rule the Commission establishes in this document. The Commission disagrees with commenters who suggest that it imposes a 90-day shot clock for resolution of such waivers. Commenters have provided no persuasive argument supporting the establishment of an arbitrary deadline for resolution of waiver requests and the Commission similarly refrains from establishing any specialized waiver requirements for the rule adopted in this document.

63. Because of the compelling interest in protecting our national security, the Commission concludes that the rule it adopts in this document should take effect immediately upon publication in the *Federal Register*. For purposes of the Lifeline and High-Cost Support Programs, any prohibition on the use of USF funds will take effect immediately upon publication of the effective date contained in the Final Designation Notice designating an entity as a covered company posing a national security threat. A requirement that USF recipients certify that they are in compliance with the Commission's rule will take effect following revision of each information collection as described in this document, including approval

by the Office of Management and Budget under the Paperwork Reduction Act

64. In the April 2018 *Protecting Against National Security Threats Notice*, the Commission made clear that its proposed rule would apply only prospectively. The Commission sought comment on how long USF recipients would need to comply with the rule and whether it should consider phasing in the rule for certain programs or USF recipients. The Commission agrees with commenters who argue that the Commission should not delay the effective date of the rule. These commenters contend that service providers have long been aware of the security risks associated with certain vendors that may affect their ability to continue to receive federal funding, and thus many service providers have already made the business decision to purchase equipment from alternative vendors, precisely to avoid the security risks and the possible greater costs those risks might present in the long run. Given the important national security concerns at stake in the proceeding, the Commission believes it is critical that it moves forward expeditiously. Moreover, because many service providers have already made the business decision to purchase equipment from alternative vendors in order to avoid security risks, the Commission believes that the impact of an immediate effective date will be minimal. Given the industry's long-standing knowledge of the risks posed by the installation and purchase of such equipment, the Commission does not believe that a phase-in period is necessary. Indeed, the important national security concerns at issue necessitate swift action.

65. Moreover, because the rule is prospective in effect, it does not prohibit the use of existing services or equipment already deployed or in use. USF recipients may continue to use equipment or services provided or produced by covered companies obtained prior to the issuance of the rule, but *may not* use USF funds to purchase, obtain, maintain, improve, modify, or otherwise support such equipment or services in any way.

66. The Commission next clarifies how its rule shall apply for E-Rate and Rural Health Care recipients. Specifically, unlike other USF recipients, E-Rate and Rural Health Care recipients apply for funding to cover specific services and equipment on coordinated basis, with funding tied to a particular funding year. To ensure prospective only effect, the rule the Commission adopts will apply to all funding

years that start after the designation of a covered company (so the Commission would expect the rule prohibiting purchases from Huawei and ZTE that it initially designates in this document to apply for Funding Year 2020, starting July 1, 2020). This provides a common administrative deadline for applicants and USAC and should allow sufficient time for E-Rate and Rural Health Care applicants to be trained to include service provider security compliance as a necessary factor in the selection of providers for the forthcoming funding year. The Commission notes that Funding Year 2020 for both programs begins July 1, 2020. The Commission believes that the decision strikes the best balance for promoting national security in a way that is practicable for E-Rate and Rural Health Care participants. For earlier funding years, the Commission directs USAC to process Operational Service Provider Identification Number (SPIN) changes and service substitutions to swap out non-compliant equipment for compliant equipment upon a showing that the equipment not yet installed would be prohibited under the Commission's rule.

67. *Existing Multiyear Contracts*. The Commission finds that its rule extends to existing contracts to acquire equipment or services from any covered company that were negotiated and entered into prior to the final designation of that entity as a covered company. In other words, existing multiyear contracts to acquire equipment or services from a covered company will not be exempt from the rule. The Commission disagrees with commenters who favor such an exemption. Exempting existing multiyear contracts would negate the purpose behind the Commission's rule and allow federal funds to be used to perpetuate existing security risks to communications networks and the communications supply chain.

68. Some commenters raise a number of constitutional challenges to the rule the Commission adopts in this document. They argue that the action adopted in this document, violates principles of due process, that it amounts to an unconstitutional bill of attainder, and that it amounts to a regulatory taking by denying carriers any economically productive use of their existing networks. The Commission finds these arguments unpersuasive.

69. Both carriers and suppliers argue that a national security condition on USF funding

would violate their due process rights guaranteed by the Fifth Amendment. The Due Process Clause of the Fifth Amendment provides that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law." These due process challenges, therefore, involve two questions: First, whether carriers or suppliers are deprived of a protected interest in "property" or "liberty." And second, if they are, whether the procedures employed by the Commission comport with principles of due process. The Commission concludes that the rule and its application, as adopted in this document and applied initially to Huawei and ZTE, do not violate the due process rights of USF recipients, of suppliers generally, or of Huawei and ZTE specifically. The Commission discusses these conclusions in the following.

70. *Carriers' Due Process Claims*. CCA, on behalf of its carrier members, argues that the rule will violate the due process rights of carriers that rely on USF support in two ways. First, CCA asserts, the rule will interfere with carriers' "long-standing investment-backed reliance interests" in their telecommunications networks. Second, CCA claims that the rule "violates the due process rights of equipment, device and service providers, as well as the carriers who rely on them" by failing to provide "an opportunity to review the unclassified evidence on which the official actor relied." Because this second argument primarily concerns the due process rights of suppliers and is also raised by them in more detail, the Commission addresses it—along with suppliers' other concerns—in the following.

71. Regarding its first argument, CCA explains that many carriers have upgraded or are upgrading their networks to the newest available technologies, including by contracting with foreign suppliers who offer competitive pricing, in service of "the USF's mandate to provide affordable telecommunications access to underserved communities." Invoking *FCC v. Fox Television Stations*, CCA argues that these carriers "did not have fair notice of what would be forbidden," and invoking *General Motors Corp. v. Romein*, CCA asserts that the proposed rule "unfairly interferes with carriers' legitimate expectations without sufficient justification."

72. In *Romein*, General Motors challenged the effect of a Michigan workers' compensation statute that required it to retroactively pay workers' compensation benefits. General Motors argued that the statute's retroactive provisions "unreasonably interfered with closed transactions," and thereby

violated due process. Applying rational basis review, the Court rejected this challenge and found that the statute was a rational means of achieving a legitimate objective. Huawei similarly argues that the rule the Commission adopts in this document would violate the Administrative Procedure Act as a rule that has "unreasonable secondary retroactivity." While the Commission acknowledges that the rule may have some retroactive effect, the Commission finds that any retroactive effect is reasonable in light of the goals of the Report and Order. Secondary retroactivity is reviewed under a reasonableness standard to determine whether or not it is arbitrary or capricious. The Commission notes that the rule and the initial designation of Huawei and ZTE as covered companies will not explicitly prevent Huawei from selling its products to any company. And as noted, the Commission concludes that multiyear contracts cannot be exempt from the rule, given that such an exemption would largely undermine the national security goals of the Report and Order.

73. At the outset, at least with respect to Huawei and ZTE, the Commission rejects the premise that carriers had a "legitimate expectation" of being able to continue to purchase products and services from them using USF funds and "did not have fair notice" that a rule like the one adopted in this document may be imposed. Mounting public concern about these entities was apparent at least as early as 2010, when a bipartisan group of lawmakers wrote a letter to the Chairman of the FCC, requesting information about the security of U.S. telecommunications networks in light of potential deals between U.S. carriers and Huawei and ZTE.

74. Moreover, CCA's reliance on *Fox Television* is misplaced. That case addressed whether the FCC had violated the due process rights of two television networks by failing to give them fair notice that, in contrast to a prior FCC policy, a fleeting expletive or a fleeting shot of nudity could be actionably indecent. Here, by contrast, the Commission has issued a *Notice* and allowed interested parties to comment on the proposed rule, which will only be applied prospectively and does not require carriers to remove or stop using any already-purchased equipment or services. This situation is materially different than that presented in *Fox Television*, and at least one court has rejected an attempt to invoke *Fox Television* under similar circumstances, where parties were given notice and an opportunity to comment

on the proposed rule. Finally, the Commission disagrees with CCA's apparent assertion that it has not provided "sufficient justification" to satisfy the test for rational basis review articulated in *General Motors*. The government has a legitimate interest in safeguarding national security, and the Commission's rule is a rational means of furthering that interest.

75. *Suppliers' Due Process Claims*. Some commenters—including Huawei—argue that due process requires that the rule offer suppliers designated as national security threats notice and a meaningful opportunity to respond to the evidence against them. Assuming that a designation could result in a deprivation of a cognizable liberty or property interest, an argument which the Commission considers and rejects in the following, the Commission has provided and will continue to provide due process as required under the Constitution and process in conformance with the Administrative Procedure Act. Under *Mathews v. Eldridge* and other applicable precedent, due process requires that the deprived party be afforded notice of the action, including enough information about the factual basis for the action to allow for a meaningful challenge, and a meaningful opportunity to be heard. An evaluation of the sufficiency of the process will consider the private interest that would be affected, the risk of an erroneous deprivation of such interest through the procedures used (and the probable value, if any, of additional procedural safeguards), and the government's interest, including the burdens of additional procedural requirements.

76. The rulemaking proceeding has provided and will continue to provide Huawei and ZTE with notice and an opportunity to be heard on the issue of whether they should be designated under the rule adopted in the Report and Order. The *Protecting Against National Security Threats Notice* in the proceeding set forth Congress's concern with both companies and explained that this concern stems from the fact that both companies are subject to such a degree of undue influence by the Chinese government as to raise counterintelligence and security concerns. It was clear from the *Protecting Against National Security Threats Notice* that the Commission was considering designating them under the proposed rule. In fact, the *Protecting Against National Security Threats Notice* specifically sought comment on "defin[ing] covered companies as those specifically barred by the National Defense Authorization Act

from providing a substantial or essential component, or critical technology, of any system, to any federal agency or component thereof," and the WCB specifically sought comment on how the 2019 NDAA should affect the Commission's approach in the proceeding. Huawei responded to the *Protecting Against National Security Threats Notice* at great length, and the Commission has fully considered those arguments. As with any Commission decision, the Report and Order is subject to procedures for reconsideration by the Commission and for judicial review.

77. Further, both Huawei and ZTE will have an additional opportunity to respond to the factual allegations supporting their initial designation under the process established in the Report and Order. The initial determination adopted in the Report and Order expands on the concerns raised in the *Protecting Against National Security Threats Notice* and responds to Huawei's submissions that attempted to address these concerns. Huawei and ZTE will have a further chance to respond before PSHSB issues a final designation that either affirms or rejects the initial designation. The Commission therefore concludes that Huawei and ZTE will be afforded all the process that is due in the proceeding.

78. For all other designations, the Commission will adhere to the process discussed in this document, which includes notice and an opportunity to comment on any initial designation, a description of the basis for such initial designation and, if opposed, a written final determination subject to review by the Commission and, ultimately, the courts. Any such designation will also be subject to review, and potentially reversal, in the future if such an entity, or another interested entity, can demonstrate that it should no longer bear such a designation.

79. Huawei is incorrect when it argues that it violates the Due Process Clause to issue this adjudicatory decision in the context of a rulemaking proceeding. There is no requirement that designations be made pursuant to the formal adjudicatory procedures of the Administrative Procedure Act. Rather, the relevant question is whether the affected parties have had the "opportunity to present, at least in written form, such evidence as those entities may be able to produce to rebut the administrative record." Huawei has already done so here, and ZTE had the same opportunity. There is nothing improper about issuing a designation pursuant to a rulemaking proceeding. Additionally, Huawei and

ZTE will have a further opportunity to specifically respond to their initial designation during the comment period adopted in the Report and Order.

80. Moreover, the Fifth Amendment guarantees due process only where government action threatens or deprives an individual of life, liberty, or property. The Commission finds that designated suppliers and/or carriers do not suffer a deprivation of life, liberty, or property sufficient to trigger due process protections. Huawei claims that designating it under the rule the Commission adopts in this document would deprive it of liberty in three related ways: (1) by interfering with its freedom to practice a chosen profession; (2) by debarring it or effectively debarring it by preventing it from selling equipment and services to USF recipients; and (3) by imposing a "stigma" sufficiently serious to alter Huawei's legal status. The Commission finds none of these arguments persuasive.

81. First, covered companies are not barred from a field of employment. Unlike the aggrieved parties in the cases cited by Huawei and CCA, the suppliers found to be a threat to national security will not be broadly excluded from a profession or field—such as aeronautics or law. To the contrary, any such designated suppliers will be free to pursue their business by serving as suppliers to a variety of carriers; in fact, as one commenter pointed out, a designation would not formally restrict them from conducting business with *any* customer, including those who participate in USF programs.

82. Second, the adopted rule does not debar covered companies, either through "formal debarment" or through "broad preclusion, equivalent in every practical sense to formal debarment." Huawei itself recognizes an uneasy fit with the debarment cases it cites, conceding that those cases "merely involve actions that preclude private entities from transacting with the Government, while the proposed rule would preclude private entities from transacting with other private entities who spend federal funds." Huawei argues, *inter alia*, that the proposed rule meets the definition of debarment in section 54.8 of the Commission's rules. Even assuming Huawei is "debarred" from the USF under this definition, it is not "debarred" as the term is used in the cases cited by Huawei, which, as Huawei itself notes, involve government actions precluding private entities from serving the government. The Commission is similarly unconvinced by Huawei's attempt to analogize itself to a subcontractor. While

there is some authority for the proposition that due process protections extend to the debarment of subcontractors, Huawei and other affected suppliers are not subcontractors, and, even if they were, designation here does amount to *de facto* debarment—it does not prevent designated suppliers from doing business with the government or carriers (the prime contractors, in Huawei's analogy).

83. The rule here does not prevent any private entity from transacting with the government—either formally or through broad preclusion equivalent to formal debarment—nor does it completely prevent entities from transacting with carriers who receive USF funding.

84. Third, designation as a covered company does not create a deprivation by imposing a stigma sufficiently serious to alter a supplier's legal status. To establish a deprivation under this "stigma-plus" theory, a party must show (1) the public disclosure of a stigmatizing claim by the government; and (2) an accompanying denial of "some more tangible interest such as employment, or the alteration of a right or status recognized by state law." With respect to the first prong, assuming *arguendo* that designation by the Commission as a threat to national security is likely to impose some amount of stigma, the stigmatized party must also satisfy the "plus" factor of the "stigma plus" test. Courts have found this factor satisfied where the government has deprived a party of some benefit to which it has a legal right, like the ability to purchase alcohol or fly. The D.C. Circuit has found this prong satisfied where the government-imposed stigma is so severe that it "broadly precludes" the stigmatized party from "pursuing a chosen trade or business." The Commission finds that the rule adopted in this document does not satisfy this prong.

85. Huawei argues that the alleged stigma of a designation under the proposed rule would alter its status in two ways. First, by "barring the use of universal service funds to buy the company's equipment." Second, by having the practical effect of discouraging other U.S. entities from buying Huawei's equipment. But while designation may create a disincentive for carriers to purchase equipment from designated entities, designation imposes no explicit restriction on designated entities at all; designated entities remain free to sell to anyone, including recipients of USF. Likewise, USF recipients remain free to purchase equipment from designated entities—and some may continue to do so, though

they would not be able to use USF support for any covered equipment and services. This fact alone would prevent Huawei or other covered companies from establishing the deprivation of a legal right or the "broad preclusion" required in *Trifax*, the case on which Huawei principally relies in establishing this factor. Thus, the Commission concludes that there is no cognizable deprivation of liberty or property either in adopting the rule or designating Huawei and ZTE herein the Report and Order.

86. *Unconstitutional Taking.* Some commenters assert that the Commission's proposed rule would constitute a regulatory taking because it would deny some carriers of "all economically beneficial or productive use" of their property." These commenters argue that the proposed rule would prevent carriers from upgrading, repairing, or servicing pre-existing equipment purchased from prohibited suppliers, rendering this equipment useless. Without funding to compensate carriers for these losses, they argue, the proposed rule will run afoul of the Takings Clause of the Fifth Amendment, which prohibits the government from taking "private property . . . for public use, without just compensation."

87. The Commission disagrees with these arguments. At the outset, the Takings Clause applies only when "property" is taken, but Commission and judicial precedent make clear that carriers have no vested property interest in ongoing USF support. Therefore, there is no merit to any suggestion that deprivation of future USF support amounts to a Takings under the Fifth Amendment. While carriers do have a cognizable property interest in their equipment, to the extent the action diminishes the value of equipment carriers have already purchased, this interference does not amount to a regulatory taking. The concurrently adopted Further Notice addresses making additional support available pursuant to NDAA section 889(b)(2)—a fact that arguably mitigates any takings concerns and makes any potential takings claim unripe. Further, there is no *per se* regulatory taking under *Lucas v. South Carolina Coastal Council*, because the rule will not deprive affected carriers of all economic value in their networks or equipment—the proposed rule is prospective in nature, and will allow them to continue using pre-existing equipment. Nor does the rule effect a partial regulatory taking under the three-factor test established in *Penn Central Transportation Company v. New York City*. First, the economic impact on affected carriers should not be severe, as they should still be able to use pre-existing equipment. Second, the rule should

not upend reasonable investment-backed expectations. As explained in this document, the long history of concern about Huawei and ZTE should have served as a warning that the federal government may take action regarding these companies, and in any event the *Protecting Against National Security Threats Notice* provided affected carriers actual notice of this action. More broadly, the Commission frequently enacts rules adjusting the levels of USF support received by carriers, and has long held that carriers have no entitlement to ongoing USF support at current levels. Third and finally, with respect to the "character" of the Commission's action, any interference could not be characterized as physically invading or permanently appropriating the property of carriers—and commenters seem to offer no argument to the contrary.

88. *Bill of Attainder*. Lastly, Huawei argues that the rule violates the Bill of Attainder Clause. A law constitutes a bill of attainder "if it (1) applies with specificity, and (2) imposes punishment." According to the Supreme Court, "the Bill of Attainder Clause was intended . . . as an implementation of the separation of powers, a general safeguard against legislative exercise of the judicial function, or, more simply, trial by legislature." Thus, "[a] bill of attainder is a legislative act which inflicts punishment without a judicial trial." Huawei argues that the rule "contravene[s] the Bill of Attainder Clause by targeting a small group of people for punitive measures."

89. The Commission finds this argument unpersuasive. First, the Supreme Court has never applied the Bill of Attainder Clause to a corporation like Huawei. Second, the rule cannot amount to a bill of attainder because it is not a "legislative act." The Commission is unaware of any court opinion applying the Bill of Attainder clause to agency regulations. In a case challenging the Commission's 2011 order overhauling the high-cost universal service program, the Tenth Circuit considered and rejected a similar argument on the grounds that the Commission's order was not a legislative act. Second, even if the rule were a "legislative act," it does not impose a "punishment." As the Report and Order makes clear, the Commission has a legitimate, non-punitive reason to take the actions contemplated by the rule—the protection of national security. While some of the burdens of the rule will fall on those entities identified as threats to national security, the burdens imposed will not be "so disproportionately severe

and so inappropriate to nonpunitive ends that they unquestionably have been held to fall within the proscription of [the Bill of Attainder Clause]."

90. The Commission's cost benefit analysis focuses on the economic costs of its action. An economic cost is the extent to which resources are spent inefficiently, in this case, on more expensive suppliers. The Commission notes that record evidence indicates the vast majority of such costs are attributable to ETCs receiving high-cost universal service support. The Commission accordingly focuses its analysis on such costs because any costs attributable to other programs are unlikely to have any measurable impact on whether the benefits of the rule outweigh its costs. Furthermore, the records suggest that the dominant economic cost equals the necessary additional cost to carriers who choose to purchase more expensive equipment as a result of the Commission's action. The Commission estimates this cost and qualitatively consider other economic costs of its action. The Commission finds these other costs to be relatively small. Given the evidence available, the Commission estimates that the costs of the actions in this document will not exceed $960 million and are likely to be much lower.

91. Quantifying the expected benefits of the Commission's rule is difficult. Nonetheless, the Commission takes into account several comparable situations to estimate an order of magnitude lower bound of benefits. Notably, a foreign adversary's access to American communications networks could result in hostile actions to disrupt and surveil our communications networks, impacting our nation's economy generally and online commerce specifically, and result in the breach of confidential data. To start, our national gross domestic product was $20.5 trillion last year, growing 2.9% or $595 billion last year, adjusting for inflation. Accordingly, preventing even a 0.005% disruption to our economy, or a 0.162% disruption to annual growth, would outweigh the costs of the prohibition. Likewise, the digital economy accounted for $1.35 trillion of our economy in 2017, and so preventing a disruption of even 0.072% would mean the benefits of the rule outweigh the costs. Given how dependent the general economy—let alone the digital economy—is on our national communications network and how interconnected that network is and is becoming, the Commission finds it likely that any potential disruption would exceed these measures by a large margin. As a check on the Commission's analysis,

consider the impact of existing malicious cyber activity on the U.S. economy: $57 billion to $109 billion in 2016. Given the incentives and documented actions of hostile nation-state actors, reducing this activity (or preventing an expansion of such damage) by even 1.68% would justify the costs of the Commission's rule. Or set aside broader commercial implications (such as theft of trade secrets and business plans) and focus on the impact of data breaches on consumers: An estimated 7% of consumers over the age of 16 were identity theft victims in 2014, and the estimated average loss to an identity theft victim is over $2,800. Accordingly, if the Commission's rule reduced the incidence of data breach and identity theft by just 0.137% among American consumers over the age of 16, the benefits of the rule would outweigh the costs. In the Commission's judgment and given this analysis, the Commission finds the benefits of its rule to the American economy, commerce, and consumers are likely to significantly and substantially outweigh the costs by a large margin (the upper end of those costs being $960 million). Finally, the Commission notes that the benefits of the rule also extend to even harder to quantify values, such as preventing untrustworthy elements in the communications network from impacting our nation's defense, public safety, and homeland security operations, our military readiness, and our critical infrastructure, let alone the collateral damage such as loss of life that may occur with any mass disruption to our nation's communications networks. The Commission finds that the benefits of safeguarding our nation against these threats alone would also significantly and substantially outweigh the costs of the Commission's rule by a large margin.

92. *Calculating the Additional Cost to Carriers*. The Commission assumes based on the initial designations that its actions will prevent a carrier from using universal service funds to make purchases from Huawei or ZTE. As carriers maintain their existing networks and upgrade them to new technologies such as 5G, carriers relying on universal service funds may choose more expensive equipment—and for the sake of this cost-benefit analysis, the Commission assumes that the prices of Huawei and ZTE tend to be lower than those of other suppliers without a corresponding loss in quality, reliability, or durability. Buying more expensive equipment or services also increases the value of the firm's capital base, which in turn, increases service and maintenance costs, and the required return on

capital to bondholders and shareholders, resulting in a second source of cost. The Commission also estimates a useful lifetime of network equipment (like mobile switches) and exterior equipment (radio network access equipment (RAN) placed on or near a pole or tower) of approximately 10 years.

93. To estimate the additional cost to carriers of the prohibition and given the estimated useful lifetime of network equipment, the Commission expects that in 10 years all Huawei and ZTE equipment that will be replaced (or upgraded) with universal service support will have been replaced. At that point, the additional annual capital outlays will peak, and the Commission generously estimates the total annual cost of its actions, including service and maintenance cost, and the required return on capital, will be between approximately $17 million and $107 million. Although the Commission initially assumes Huawei and ZTE maintain their (non-quality-adjusted) price advantage for 10 years, the Commission then allows competition to linearly eliminate that advantage over the next ten years. On that basis, the Commission estimates the present value of the cost this will impose on carriers to range from $160 million and $960 million.

94. The analysis assumes constant real equipment prices. While real equipment prices will likely decline, it is the difference between the prices of alternatives to Huawei and ZTE equipment and the prices of Huawei and ZTE equipment that determines the reimbursement cost. While lower real prices would increase demand, they would also reduce the extent to which reimbursements from the Fund are necessary, the net effect of which is likely to be small relative to the error inherent in the Commission's estimates.

95. In developing these estimates, the Commission first estimates the cost of replacing Huawei and ZTE equipment, and then estimate ongoing expenses. Since the Commission's Report and Order does not mandate replacement, the Commission does not assume that all Huawei and ZTE equipment is replaced by alternative equipment. Instead, the Commission expects that a fraction of the Huawei and ZTE equipment will be replaced. The Commission then estimates the ongoing expenses implied by the assumed replacements. However, the sum of the estimated replacement and ongoing costs is not entirely attributable to the Commission's action. Instead, it is the difference between these costs

and the costs that would have been incurred if Huawei and ZTE equipment were used. The Commission estimates this difference using reported differences between the prices of Huawei and ZTE equipment and the prices of alternative equipment (again, setting aside for these purposes concerns about the lower quality, reliability, or durability of such lower-priced equipment).

96. The Commission estimates the average cost for a firm to replace its Huawei and ZTE equipment, excluding ongoing expenses, to range from $40 million to $45 million. The Commission then multiplies this by an estimate of the number of firms that have Huawei or ZTE equipment and relies on universal service support, and then reduces it to account for the extent to which carriers will use other sources of capital to purchase and maintain Huawei and ZTE equipment. The result is an estimate of the cost of replacing Huawei and ZTE equipment, excluding ongoing expenses.

97. Seven carriers reported their estimated cost of replacing installed Huawei or ZTE equipment. The estimates come from Pine Belt Cellular, Sagebrush, Union Telephone Company, NE Colorado Cellular, SI Wireless, United TelCom, and James Valley Telecommunications. The median of the firms' replacement cost estimates is $50 million.

98. To guard against distortion due to extreme estimates, particularly given carriers' incentives to report higher estimates, the Commission prefers the median to the mean. The mean of the 7 reports, $94 million, is significantly raised by NE Colorado Cellular's cost estimate, which is 3 times larger than the next highest estimate, and 60 times larger than the lowest estimate. NE Colorado Cellular's absolute costs also seem high. It reports 80% of its network to be Huawei equipment, which it estimates would cost $360 million to replace. That implies a network with a replacement cost of approximately $450 million (= $360 million/0.8 million). Assuming an annual cost factor of 25%, this implies annual expenses of $112.5 million. As a comparison, the annual cost of switching in the Connect America Model is 0.2671, the sum of the annual charge factors for capital expenditures, 0.1476, and operating expenditures, 0.1195. (For the Commission's estimates of the Report and Order costs, the Commission uses a 30% annual charge factor, as it wishes to avoid understating the costs of its actions. Here, the Commission seeks to show that NE Colorado Cellular's costs are high, so it uses a 25% annual

charge factor to demonstrate that their reported costs are high even under conservative assumptions.) NE Colorado Cellular reports serving 110,000 customers, so capital costs alone amount to approximately $85 per month per customer ($112.5 million/12/110,000 = $85). Of course, NE Colorado Cellular must recover costs beyond its capital costs. NE Colorado Cellular collects and pays roaming fees, the net of which could reduce the required monthly recovery from its customers, but presumably not radically. Thus, NE Colorado Cellular would need to be charging monthly subscriber fees of around or probably in excess of $85 per month, which seems high, especially compared with T-Mobile's "Premium Unlimited Plan," which costs $50 per month per subscription when four subscriptions are purchased.

99. The Commission expects that firms motivated to report their costs in the record of the proceeding have above average costs. Indeed, the reporting carriers are unlikely to be representative of carriers affected by the Commission's actions, but rather reflect carriers with greater incentives to put their concerns in the record, i.e., carriers for which the impact of a rip-and-replace requirement is large compared with similarly situated non-reporting carriers. In 2018, the 7 carriers who provided rip and replace cost estimates represented only 0.15% of mobile carrier end-user revenues as reported in their FCC Form 499s. Consequently, the Commission conservatively discounts the median of reported costs by between 10% and 20%, which yields an estimated replacement cost for each network of $40 million to $45 million.

100. The Commission generously estimates 106 firms currently buy Huawei and ZTE equipment. Huawei reports serving 85 U.S. customers in 2019. Alternatively, the Commission could rely on the Dell'Oro Group's North American market share estimate for ZTE of zero. This would imply only 85, rather than 106 purchasers, lowering the Commission's cost estimates by approximately 20%. Market share estimates for Huawei and ZTE, respectively of 31.1% and 7.5%, imply 105.5 (= 85*(1 + 7.5/31.1)) purchasers of equipment from Huawei and ZTE. *See* Dell'Oro Group, Market Research Reports on Mobile Radio Access Network, which also finds Huawei's North American share to be only 1.5% and ZTE's to be zero. This is likely an overestimate as both suppliers, but especially ZTE, have experienced a decline in their U.S. customer bases. For sake of this analysis, however, the Commission rounds up to

106 firms. Given all of these customers are not likely to be ETCs, e.g., they may be firms purchasing Wi-Fi routers for internal use, the Commission estimates between 32 (30%) and 53 (50%) of these firms accept universal service funds. This range is consistent with CoBANK's estimate that 30 rural carriers are impacted.

101. Lastly, the Commission recognizes capital is fungible, and carriers have some leeway to buy Huawei or ZTE equipment from other funding sources. For these carriers, the Commission estimates they may only use universal service funds to replace between 50% and 75% of their existing Huawei or ZTE equipment. The Commission's actions prevents carriers from purchasing Huawei and ZTE equipment using universal service funds but does not prohibit them from purchasing such equipment using funds from other sources so long as they can meet the accounting requirements described in this document. This gives the following lower and upper bounds for the costs of replacing installed Huawei or ZTE equipment:

Lower bound: $640 million = $40 million*32*50%.

Upper bound: $1.79 billion = $45 million*53*75%.

102. *Converting the Replacement Cost into a Cost Stream*. Assuming the average useful life of the equipment in question is ten years, then on average in each year, 10% of the total value of the equipment must be replaced. The Commission adds to this an additional 20% of the value of the equipment for expenses for service and maintenance costs and a return to bondholders and shareholders. The sum equals a generous annual charge factor of 30%. This may be broken down into a 10% factor for capital purchases to maintain the capital base, and a 20% factor for service, maintenance, and a return to bondholders and shareholders. By comparison, the annual cost factor for switching in the Connect America Model is 0.2671 the sum of the annual cost factors for capital expenditures, 0.1476, and operating expenditures, 0.1195. This, with assumptions about prices discussed in this document, allows the Commission to develop a cost stream associated with each year for 20 years.

103. *Comparing Expenses under the Report and Order with the Case of No Report and Order*. Of course, this equipment would be replaced with or without the Commission's requirement. The

relevant cost of the Commission's action is the price differential or markup between purchasing alternative equipment and Huawei or ZTE equipment. Sources suggest this markup ranges from 5% to 40% (not taking into account any change in quality, reliability, or durability). These markups do not account for quality differences between Huawei and ZTE, and their rivals, or the likelihood that these rivals' prices will become more competitive over time. The 40% estimate, which is well above the other two estimates, comes from a carrier that appears particularly concerned about the Commission's actions, and hence may have overestimated the markup. Consequently, the Commission uses the mid-points of each of the other two markup estimates, 10% and 25%, as lower and upper bounds. Using these price markup assumptions and subtracting the annual cost streams in the absence of the Report and Order from the cost streams under the Report and Order results in a stream of cost differences. The Commission thus estimates the present value of the cost differences for the next twenty years that would arise due to the Report and Order ranges from $160 million to $960 million.

104. *The Economic Efficiency Costs of the Commission's Actions*. So far, the Commission has only discussed the replacement cost of its actions. To understand the potential breadth of the economic cost of the Commission's actions, first consider the simple case in which prices of both the cheaper and the more expensive providers recover no more than the economic costs of supply, including a return of capital (capital replacement), and a return on capital, accounting for the risks the firm's owners bear. Call this a normal profit. In that case, the cost just calculated is a key economic cost, representing an increase in resources used because the Commission's actions cause carriers to shift their purchases from more to less efficient providers. But there is a further efficiency consequence of the Commission's actions. Purchase from less efficient suppliers occurs at higher (quality-adjusted) prices. If the quality-adjusted prices of Huawei and ZTE are equal to their rivals' prices, then the Commission's actions would have no costs. However, some carriers prefer Huawei or ZTE to alternative suppliers, implying that these carriers view the prices of Huawei or ZTE to be the lowest quality-adjusted price available to them. This lowers output because end users face higher prices, and consequently purchase less than is efficient. Estimating the efficiency cost of this is difficult, but relative to the replacement cost, the distortion cost is small and

likely swamped by the error inherent in the replacement cost estimate. This is true from a global as well as a domestic perspective.

105. This can be seen by focusing on the intermediary market for network equipment, i.e., demand in this market is derived from demand for services provided to end users. This implies the distortions in the intermediary market reflect those in the final market. The reimbursement cost to the Universal Service Fund is the product of the amount of network equipment bought and sold at the new higher prices, call this Q, and the markup over Huawei and ZTE prices, call this ΔP. The cost of the distortion caused by the reduction in demand for network equipment due to inefficiently higher prices is the lost value consumers would have obtained from the additional quantity they would have consumed at the Huawei or ZTE prices. This lost value equals the area under the demand curve in the region where demand is curtailed due to the higher prices of the alternative suppliers. At a first approximation, this cost is, because demand is downward sloping, strictly less than the product of the change in what is bought and sold, call this ΔQ, and the change in price, ΔP. The reimbursement cost, $\Delta P*Q$, swamps the distortion cost, $\Delta P*\Delta Q$, since Q is generally considerably larger than ΔQ. Thus, if higher prices reduce demand by 5% ($= \Delta Q/Q$), then the distortion cost could not add more than 5% to the cost to the Universal Service Fund ($\Delta P*\Delta Q/\Delta P*Q = 5\%$).

106. From a global perspective, the Commission's estimates of the economic cost of its actions would be higher to the extent that Huawei or ZTE earn more than a normal profit despite having substantially lower prices than their rivals. Purchases diverted to alternative suppliers would cause Huawei and ZTE to forgo that extra-normal profit. However, it seems unlikely that Huawei or ZTE earn extra-normal profit. Similarly, from a global perspective, the Commission's economic cost estimate would be lower to the extent that the prices of the rivals of Huawei and ZTE, today essentially being Ericsson and Nokia, incorporate extra-normal profits. While U.S. purchasers, and hence the Universal Service Fund, would be spending more when purchasing from Ericsson and Nokia at higher prices, to the extent these prices incorporate extra-normal profit, this would be a transfer from the U.S. to the foreign owners of Ericsson and Nokia. Finally, from a global perspective, if Huawei or ZTE's prices are less than

what is required to recover their costs of operations, e.g., due to a government subsidy, then the economic cost of the Commission's actions would be lower.

107. The Commission rejects Huawei's claims that its actions would reduce 5G deployment and would materially increase mobile radio access network equipment prices in the U.S., which in turn would materially harm growth and employment in the U.S. economy. It is unlikely the Commission's actions will impact U.S. 5G deployment. The four largest U.S. mobile carriers do not use and have no plans to use Huawei (or ZTE) radio access network equipment. Given this, and Aron's claim that there are high costs associated with switching from one equipment manufacturer to another, it is implausible that the Commission's actions will affect these carriers' 5G deployment plans. More broadly, the Commission finds it unlikely that its actions will materially increase U.S. radio access network equipment prices. While carriers that buy equipment from covered companies could face higher prices in the near term (and only to the extent they use universal services funds to purchase that equipment), Huawei's own chief executive has admitted that Huawei has "virtually no business dealings in the U.S."—making it far more likely that the Commission's rule will have "virtually no" impact on 5G deployment. What is more, the Commission finds that ensuring a robust ecosystem of trusted vendors for 5G equipment (one collateral consequence of the Commission's rule) is more likely to keep 5G equipment prices checked by a competitive market over the long term, facilitating deployment and continued U.S. leadership in 5G.

III. INFORMATION COLLECTION ORDER

108. In the concurrently adopted Further Notice, the Commission seeks comment on proposals to address the national security threats arising from the existing use of equipment or services produced or provided by covered companies. To support the Commission's future efforts to protect the communications supply chain, the Commission directs WCB and OEA, in coordination with USAC, to conduct an information collection to determine the extent to which potentially prohibited equipment exists in current networks and the costs associated with removing such equipment and replacing it with equivalent equipment. The information collection will aid the Commission's review of the record and guide its next steps in the proceeding. Because section 889(f) of the 2019 NDAA identifies specific

companies that are prohibited from federal procurements, and the concurrently adopted Further Notice seeks comment on how to implement those and other prohibitions, the Commission specifically seeks comment on the extent to which equipment or services from companies identified in Section 889 of the NDAA exist in current networks.

109. The Commission seeks information from ETCs on the potential costs associated with the complete removal and replacement of any equipment and services produced or provided by Huawei and ZTE. The information collection applies to all subsidiaries and affiliates of ETCs.

110. Specifically, the Commission seeks information on all equipment and services from Huawei and ZTE that are used or owned by ETCs. ETCs are the subject of the Commission's proposed rule (and among USF recipients the most likely to currently own and use equipment and services from Huawei and ZTE). The Commission therefore limits its information collection only to ETCs and will not require cost information from other USF recipients at this time. The Commission nonetheless will allow service providers that are not ETCs to participate on a voluntary basis should they have ETC designation petitions pending (or may intend to file such in the future). And the Commission will allow other USF recipients who are not ETCs to participate on a voluntary basis as well.

111. In implementing the information collection, WCB and OEA should gather information from ETCs as to whether they own equipment or services from Huawei or ZTE, what that equipment is and what those services are, the cost to purchase and/or install such equipment or services, and the cost to remove and replace such equipment or services. ETCs must demonstrate how they arrived at any cost estimates they provide in response to the information collection. All submissions must be certified to ensure the accuracy of the responses.

112. The information collection shall be mandatory for all ETCs and voluntary for others. The Commission directs WCB to consider the potential confidentiality of any information submitted, particularly where public release of such information could raise security concerns (e.g., granular location information). The Commission expects, however, that the public interest in knowing whether a carrier uses equipment or services from Huawei or ZTE would significantly outweigh any interest the carrier

would have in keeping such information confidential. As part of the information collection, the Commission directs WCB and OEA to seek any information necessary to verify responses provided by ETCs to the information collection, including by requiring further information from respondents. The Commission directs WCB and OEA to proceed expeditiously with the information collection, including by seeking emergency PRA approval from OMB, if necessary and appropriate. The Commission believes there is good cause for requesting emergency PRA approval from OMB for the reasons described in the following. Given the nature of the national security concerns, the Commission finds that the serious and immediate risks to communications networks likely justify the expedited approval of the information collection.

IV. PROCEDURAL MATTERS

A. Paperwork Reduction Act

113. This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in the proceeding. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), the Commission previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

B. Congressional Review Act

114. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. 804(2), because it is promulgated under the Telecommunications Act of 1996 and the amendments made by that Act. The Commission will send a copy of this Report and Order, Further Notice of Proposed Rulemaking, and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

115. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Protecting Against National Security Threats Notice* for the proceeding. The Commission sought written public comment on the proposed rule in the *Protecting Against National Security Threats Notice*, including comment on the IRFA. The Commission received only a single comment on the IRFA. Because the Commission amends its rules in the Report and Order, the Commission has included the Final Regulatory Flexibility Analysis (FRFA). The present FRFA conforms to the RFA.

116. Consistent with the Commission's obligation to be responsible stewards of the public funds used in USF programs and increasing concern about ensuring communications supply chain integrity, the Order adopts a rule that restricts universal service support from being used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.

117. The RFA directs agencies to provide a description and, where feasible, an estimate of the number of small entities that may be affected by the final rules adopted pursuant to the Order. 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. *See* 5 U.S.C. 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. 632). Pursuant to 5 U.S.C. 601(3), 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*." A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

118. *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.

119. 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).

120. 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 2012 Census of Governments indicates that there were 90,056 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number there were 37, 132 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,184 special purpose governments (independent school districts and special districts) with populations of less than 50,000. The 2012 U.S. Census Bureau data for most types of governments in the local government category show that the majority of these governments have populations of less than 50,000. Based on this data the Commission estimates that at least 49,316 local government jurisdictions fall in the category of "small governmental jurisdictions."

121. Small entities potentially affected by the rules herein include Schools and Libraries, Healthcare Providers, Providers of Telecommunications and other Services, Internet Service Providers and Vendors and Equipment Manufacturers.

122. *Restriction on Use of USF Funds*. The Order adopts a rule that no universal service support may be used 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. Applicants may continue to use their own funds to upgrade and maintain such equipment. They must, however, be able to affirmatively demonstrate that they have not used any funds obtained via the USF to purchase, obtain, maintain, improve, modify, or otherwise support equipment or services provided or manufactured by a covered company. This restriction applies to any and all equipment and services, including software, produced or provided by a covered company. Because the rule is prospective in effect, it does not prohibit the use of existing services or equipment already deployed or in use. USF recipients may seek waivers of the requirements.

123. *Covered Companies*. The Report and Order initially designates Huawei and ZTE as covered companies for purposes of the prohibition the Commission adopts in this document. Independently, the Order establishes a process for designating entities as national security threats for purposes of the Commission's rule, and delegates to the PSHSB the authority to implement this process, as well as the next steps in the designation processes for Huawei and ZTE. Because equipment from subsidiaries, parents, and affiliates pose the same risks to network integrity as equipment directly from the covered company, the Commission includes any subsidiary, parent, or affiliate of a covered company as a covered company subject to the Commission's prohibition.

124. *Effective Date of Rule*. Because of the compelling interest in protecting our national security, the Commission concludes that the rule it adopts in this document should take effect immediately upon publication in the *Federal Register*. For purposes of the Lifeline and High-Cost Support Programs, any prohibition on the use of USF funds will take effect immediately upon publication of the effective date contained in the Final Designation Notice designating an entity as a covered company posing a national security threat. A requirement that USF recipients certify that they are in compliance with the Commission's rule will take effect following revision of each information collection as described in the Order, including approval by the Office of Management and Budget (OMB) under the

Paperwork Reduction Act. For E-Rate and Rural Health Care Recipients, the rule the Commission adopts will apply to all funding years that start after the designation of a covered company. The Commission's rule extends to existing contracts to acquire equipment or services from any covered company that were negotiated and entered into prior to the final designation of that entity as a covered company. In other words, existing multiyear contracts to acquire equipment or services from a covered company will not be exempt from the rule.

125. *Compliance Certifications*. The Order establishes that the Commission should require recipients of universal service support to provide a certification that they have complied with the adopted rule, and directs WCB, in coordination with USAC, to revise the relevant information collections for each of the four USF programs to implement a certification attesting to compliance with the adopted rule.

126. *Audits and Recovery of Funds*. The Order directs USAC to implement audit procedures for each USF program consistent with the adopted rule. USF recipients must be able to affirmatively demonstrate that no universal service funds were used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services provided or manufactured by covered companies. The Order notes that applicants in the E-rate and Rural Health Care programs already retain and provide information either during the application process or during audit and program integrity assurance processes that could demonstrate (if verified) that no USF funds were improperly used. And many ETCs receiving High Cost funding now report the projects they complete using federal funds to the High Cost Universal Broadband portal, allowing relatively swift verification by USAC of compliance. To the extent that other ETCs do not yet report information to USAC that would verify compliance, the Commission directs WCB and USAC to revise its information collection and audit procedures to ensure the reporting of USF expenditures in a manner that will allow efficient oversight and thorough compliance. The Order does not depart from the requirement that directs USAC to pursue recovery actions against the party or parties that committed the rule or statutory violation in question, recognizing that, in some instances, this could be the applicant school, library, health care provider, or consortium, rather than the service provider.

127. *Information Collection*. The Information Collection Order directs WCB and OEA, in coordination with USAC, to conduct an information collection to determine the extent to which potentially prohibited equipment exists in current networks and the costs associated with removing such equipment and replacing it with equivalent equipment. Specifically, the information collection will seek information from ETCs on the potential costs associated with the complete removal and replacement of any equipment and services produced or provided by Huawei and ZTE. Specifically, the Commission seeks information on all equipment and services from Huawei and ZTE that are used or owned by ETCs. ETCs are the subject of the Commission's proposed rule (and among USF recipients the most likely to currently own and use equipment and services from Huawei and ZTE). The Commission therefore limits its information collection only to ETCs and will not require cost information from other USF recipients at this time. The Commission nonetheless will allow service providers that are not ETCs to participate on a voluntary basis should they have ETC designation petitions pending (or may intend to file such in the future). And the Commission will allow other USF recipients who are not ETCs to participate on a voluntary basis as well.

128. In implementing the information collection, WCB and OEA should gather information from ETCs as to whether they own equipment or services from Huawei or ZTE, what that equipment is and what those services are, the cost to purchase and/or install such equipment or services, and the cost to remove and replace such equipment or services. ETCs must demonstrate how they arrived at any cost estimates they provide in response to the information collection. All submissions must be certified to ensure the accuracy of the responses. The information collection shall be mandatory for all ETCs and voluntary for others. The information collection applies to all subsidiaries and affiliates of ETCs. The Information Collection Order directs WCB to consider the potential confidentiality of any information submitted, particularly where public release of such information could raise security concerns (e.g., granular location information). The Commission expects, however, that the public interest in knowing whether a carrier uses equipment or services from Huawei or ZTE would significantly outweigh any interest the carrier would have in keeping such information confidential. As part of the information

collection, the Commission directs WCB and OEA to seek any information necessary to verify responses provided by ETCs to the information collection, including by requiring further information from respondents. The Commission directs WCB and OEA to proceed expeditiously with the information collection, including by seeking emergency PRA approval from OMB, if necessary and appropriate.

129. The RFA requires an agency to describe the steps the agency has taken to minimize the significant economic impact on small entities of the final rule, consistent with the stated objectives of the applicable statutes, including a statement of the factual, policy, and legal reasons in support of the final rule, and why any significant alternatives to the rule considered by the agency and which affect the impact on small entities were rejected.

130. The scope of the rule adopted in the Order is carefully limited so as to lessen its impact on small entities. Because the rule is prospective in effect, it does not prohibit the use of existing services or equipment already deployed or in use. USF recipients may continue to use equipment or services provided or produced by covered companies obtained prior to the issuance of the rule, although they may not use USF funds to purchase, obtain, maintain, improve, modify, or otherwise support such equipment or services in any way. Recipients may also continue to use their own funds to upgrade and maintain such equipment, so long as they do not use USF funds to do so. The Order also permits USF recipients to seek a waiver of the requirements. In these ways, the Order seeks to minimize the economic burden of these rules on small entities.

131. *Effective Date*. The rules adopted herein and the initial designations of Huawei and ZTE as covered companies shall be effective immediately upon publication in the *Federal Register*.

132. While a rule ordinarily will take effect 30 days after publication in the *Federal Register*, the Commission finds here that good cause exists to expedite the implementation of these rules and to make them effective upon publication in the *Federal Register*. In finding that good cause exists, the Commission applies the test articulated by the D.C. Circuit in *Omnipoint Corporation v. FCC*, which requires an agency to "balance the necessity for immediate implementation against principles of fundamental fairness which require that all affected persons be afforded a reasonable amount of time to

prepare for the effective date of its ruling."

133. The Commission first examines the necessity for immediate implementation. The record before the Commission establishes that the nature of today's communications networks is such that untrusted participants in the supply chain pose a serious and immediate risk to the integrity and proper functioning of these networks. In addition, expediting the Commission's process for analyzing such risks serves to minimize the scope of exposure of USF recipients to the significant flaws in their networks from future installation of equipment that may compromise the security of these networks, and any resulting need to replace such equipment. Against this critical national security concern the Commission balances the concerns of fairness to affected parties—including whether dispensing with the 30-day waiting period will deprive affected parties of "a reasonable time to adjust their behavior before the final rule takes effect." Here, the Commission notes that the principal effect of the rules adopted in the Report and Order—restriction on the spending of USF to certain suppliers designated as a threat to national security—will not take effect until an entity is actually designated as a threat to national security under the proposed rules. Thus, no entity will be designated until—at the earliest—31 days after the effective date of the Report and Order. In other words, making these rules effective immediately upon publication in the *Federal Register* will not inhibit any party's ability to "prepare for [their] effective date" because the rules the Commission adopts in this document does not include any requirements with which USF recipients must immediately comply.

134. While the Commission has adopted initial designations of Huawei and ZTE as covered companies, use of USF support to procure or otherwise support equipment or services produced or provided by these two companies has not and will not be disallowed until such time as PSHSB issues a public notice announcing its final determination and the effective date of any potential final designation of one or both of these companies. To the extent that accelerating the effective date requires these companies to respond more quickly to their initial designation, the Commission will provide copies of the Report and Order to both parties or their U.S. agents or affiliates immediately after release. The

Commission has recognized that a finding of good cause under section 553(d)(3) can be further supported where "the Commission is serving those entities by overnight mail."

135. Even were the rules the Commission adopts in this document to have an immediate impact on USF recipients, it does not believe it would affect the Commission's findings here. Many service providers have already made the business decision to purchase equipment from alternative vendors in order to avoid security risks. Given this, and the industry's long-standing knowledge of the risks posed by the installation and purchase of such equipment, the Commission believes that the impact of an immediate effective date would be minimal.

136. In this case, given the critical security concerns at issue, and the fact that an expedited schedule will not impede the ability of interested parties to prepare for the implementation of the rules the Commission adopts in this document, it finds that good cause exists, in accordance with the balancing test articulated by the Court in *Omnipoint*, to expedite the implementation of these rules and to make them effective immediately upon publication in the *Federal Register*.

137. Ex Parte Presentations. This proceeding shall be treated as 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.

V. ORDERING CLAUSES

138. Accordingly, IT IS ORDERED, pursuant to in sections 1-4, 201(b), 229 and 254 of the Communications Act of 1934, as amended, and section 105 of the Communications Assistance for Law Enforcement Act, 47 U.S.C. 151-154, 201(b), 229, 254, 1004, that the Report and Order IS ADOPTED.

139. IT IS FURTHER ORDERED that Part 54 of the Commission's rules IS AMENDED as set forth in the following.

140. IT IS FURTHER ORDERED that, pursuant to §§ 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR 1.4(b)(1), 1.103(a), the Report and Order SHALL BE EFFECTIVE immediately upon publication of the Report and Order in the *Federal Register*.

141. IT IS FURTHER ORDERED that, pursuant to §§ 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR 1.4(b)(1), 1.103(a), the initial designations adopted in this order SHALL BE EFFECTIVE immediately upon publication of the Report and Order in the *Federal Register*.

142. IT IS FURTHER ORDERED, pursuant to sections 1-4, 201(b) and 254 of the Communications Act of 1934, as amended, 47 U.S.C. 151-154, 201(b), 254, that the Information Collection Order IS ADOPTED. Information collection pursuant to the Order SHALL BE EFFECTIVE immediately upon OMB approval.

List of Subjects in 47 CFR Part 54

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

FEDERAL COMMUNICATIONS COMMISSION

Katura Jackson,
Federal Register Liaison Officer
Office of the Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 part 54 as follows:

PART 54 – UNIVERSAL SERVICE

1. 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, and 1302 unless otherwise noted.

2. Add § 54.9 to subpart A to read as follows:

§ 54.9 Prohibition on use of funds.

(a) *USF support restriction* No universal service support may be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.

(b) *Designation of Entities Subject to Prohibition*. (1) When the Public Safety and Homeland Security Bureau (PSHSB) determines, either sua sponte or in response to a petition from an outside party, that a company poses a national security threat to the integrity of communications networks or the communications supply chain, PSHSB shall issue a public notice advising that such designation has been proposed as well as the basis for such designation.

(2) Upon issuance of such notice, interested parties may file comments responding to the initial designation, including proffering an opposition to the initial designation. If the initial designation is unopposed, the entity shall be deemed to pose a national security threat 31 days after the issuance of the notice. If any party opposes the initial designation, the designation shall take effect only if PSHSB determines that the affected entity should nevertheless be designated as a national security threat to the integrity of communications networks or the communications supply chain. In either case, PSHSB shall issue a second public notice announcing its final

designation and the effective date of its final designation. PSHSB shall make a final designation no later than 120 days after release of its initial determination notice. PSHSB may, however, extend such 120-day deadline for good cause.

(3) PSHSB will act to reverse its designation upon a finding that an entity is no longer a threat to the integrity of communications networks or the communications supply chain. A designated company, or any other interested party, may submit a petition asking PSHSB to remove a designation. PSHSB shall seek the input of Executive Branch agencies and the public upon receipt of such a petition. If the record shows that a designated company is no longer a national security threat, PSHSB shall promptly issue an order reversing its designation of that company. PSHSB may dismiss repetitive or frivolous petitions for reversal of a designation without notice and comment. If PSHSB reverses its designation, PSHSB shall issue an order announcing its decision along with the basis for its decision.

(4) PSHSB shall have discretion to revise this process or follow a different process if appropriate to the circumstances, consistent with providing affected parties an opportunity to respond and with any need to act expeditiously in individual cases.

[FR Doc. 2019-27610 Filed: 1/2/2020 8:45 am; Publication Date: 1/3/2020]