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

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89
	)	
Huawei Designation	)	PS Docket No. 19-351
	)	
ZTE Designation	)	PS Docket No. 19-352
	)	

REPORT AND ORDER, FURTHER NOTICE OF PROPOSED RULEMAKING, AND ORDER

Adopted: November 22, 2019 **Released: November 26, 2019**

Comment Date: [30 days after date of publication in the Federal Register]
Reply Comment Date: [60 days after date of publication in the Federal Register]

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

TABLE OF CONTENTS

APPENDIX C – FINAL REGULATORY FLEXIBILITY ANALYSIS
APPENDIX D – INITIAL REGULATORY FLEXIBILITY ANALYSIS
APPENDIX E – CLASSIFIED SUPPLEMENT

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 we protect 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. Today, we build on these efforts, consistent with concurrent Congressional and Executive Branch actions, and ensure that the public funds used in the Commission's Universal Service Fund (USF or the Fund) are not used in a way that undermines or poses a threat to our national security. Specifically, in this Report and Order, we adopt 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, we initially designate Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of this rule and establish a process for designating additional covered companies in the future.

3. In the accompanying Further Notice of Proposed Rulemaking, we seek comment on additional actions to address national security threats to USF-funded networks. These include a proposal to require USF recipients that are eligible telecommunications carriers (ETCs) to remove and replace existing equipment and services produced or provided by covered companies. Additionally, we adopt an information collection to help determine the extent to which equipment and services produced or provided by covered companies exist in our communications networks.

4. Given our oversight of the USF programs that fund voice and broadband networks and services and our obligation to be responsible stewards of the public funds that subsidize those programs, we have a specific, but important, role to play in securing the communications supply chain. We believe that the steps we take today 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 our actions, along with those taken by other Executive Branch agencies, will go far in securing our nation's critical telecommunications infrastructure.

II. BACKGROUND

5. Modern communications networks are an integral component of the U.S. economy, enabling the connectivity and information exchange underlying the operations of businesses, public safety organizations, and government.[1] But these networks are vulnerable to various forms of surveillance and attack that can lead to denial of service, and loss of integrity and confidentiality of network services.[2]

[1] *Cf.* Department of Homeland Security, CISA, Infrastructure Security, Critical Infrastructure Sectors, Communications Sector, https://www.dhs.gov/cisa/communications-sector.

[2] *See* Agubor C.K., Chukwudebe G.A., and Nosiri, O.C., Department of Electrical and Electronic Engineering, Federal University of Technology, "Security Challenges to Telecommunication Networks: An Overview of Threats and Preventive Strategies," 2015 International Conference on Cyberspace Government, at 1 (Nov. 4-7, 2015), https://www.researchgate.net/publication/301649544_Security_Challenges_to_Telecommunication_Networks_An_Overview_of_Threats_and_Preventive_Strategies.

With the proliferation of ubiquitous broadband, mobile devices, and the Internet of Things, threats to our nation's networks have only increased.

6. Over the last decade, Congress and the Executive Branch have repeatedly stressed the importance of identifying and eliminating potential security vulnerabilities in communications networks and their supply chains. As early as October 2010, a bipartisan group of lawmakers expressed concern to the FCC about ensuring the security of U.S. telecommunications networks in light of potential deals between U.S. telecommunications carriers and two Chinese telecommunications equipment manufacturers, Huawei and ZTE.[3] Specifically, the lawmakers stated, "We are very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military, which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications networks so that communications can be disrupted, intercepted, tampered with, or purposely misrouted."[4]

7. In October 2012, the House Permanent Select Committee on Intelligence released a bipartisan report assessing the counterintelligence and security threat posed by Chinese telecommunications companies operating in or providing equipment to customers in the United States.[5] This report focused specifically on "Huawei and ZTE, the top two Chinese telecommunications equipment manufacturers,"[6] noting that both companies have "histories that include connections to the Chinese government."[7] The report concluded by recommending that U.S. government agencies and federal contractors "exclude ZTE or Huawei equipment in their systems," and "strongly encouraged" private-sector entities "to consider the long-term security risks associated with doing business with either Huawei or ZTE for equipment or services" and "to seek out other vendors for their projects."[8]

8. In February 2013, the White House issued Presidential Policy Directive 21 (PPD 21), which established "national policy on critical infrastructure security and resilience."[9] PPD 21 directed federal agencies to exercise their authority and expertise to partner with other agencies to identify vulnerabilities in communications infrastructure and to work "to increase the security and resilience of critical infrastructure within the communications sector."[10] It further determined that "[t]he Federal Government . . . has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner

[3] Letter from Senator Jon Kyl et al. to Hon. Julius Genachowski, Chairman, FCC, Oct. 19, 2010.

[4] *Id.*; *see also* Letter from Representative Anna Eshoo to Hon. Julius Genachowski, Chairman, FCC, Nov. 2, 2010 (expressing "grave concerns about the implications of foreign-controlled telecommunications infrastructure companies providing equipment to the U.S. market" and particular concern that "Huawei and ZTE, Chinese telecommunications infrastructure manufacturers are looking to increase their presence in the U.S.").

[5] Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE at iv (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (*2012 HPSCI Report*).

[6] *Id*. at v.

[7] *Id*. at 8.

[8] *Id*. at vi.

[9] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-criticalinfrastructure-security-and-resil.

[10] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-criticalinfrastructure-security-and-resil.

effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators."[11]

9. That same year, the U.S. Government Accountability Office (GAO) released a report assessing the potential security risks of foreign-manufactured equipment in commercial communications networks and detailing the efforts of the federal government to address the risks posed by such equipment.[12] In noting the risks to the communications supply chain, the GAO found that "[a] potential enemy or criminal group has a number of ways to potentially exploit vulnerabilities in the communications equipment supply chain, such as placing malicious code in the components that could compromise the security and resilience of the networks."[13]

10. In May 2017, the White House released Executive Order 13800, which emphasized the importance of the security of federal networks and critical communications infrastructure.[14] More specifically, Executive Order 13800 directed the Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and all other appropriate agency heads, to identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities, and to determine how best to support cybersecurity risk management efforts.[15] Executive Order 13800 further directed the Secretary of Commerce and the Secretary of Homeland Security to identify and promote action by appropriate stakeholders to "improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks."[16]

11. In December 2017, a group of 18 Senators and Representatives expressed their concerns about the security of the communications supply chain in a letter to Chairman Pai. They not only highlighted the *2012 HPSCI Report*'s finding that "Huawei . . . cannot be trusted to be free of foreign state influence and thus poses a security threat to the United States and to our systems,"[17] but echoed the

[11] Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-criticalinfrastructure-security-and-resil.

[12] Mark L. Goldstein, Director, Physical Infrastructure Issues, U.S. Government Accountability Office, Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment at i, 5 (May 21, 2013), https://www.gao.gov/assets/660/654763.pdf (noting that "other countries – such as Australia, India, and the United Kingdom – are similarly concerned about the emerging threats to their commercial communications networks posed by the global supply chain and have taken actions to improve their ability to address this security challenge") (*2013 GAO Supply Chain Report*).

[13] *Id*. at 3.

[14] Executive Order 13800 § 2(b), 82 Fed. Reg. 22391, 22393, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executiveorder-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[15] *See* Executive Order 13800 § 2(b), 82 Fed. Reg. 22391, 22393, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executiveorder-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[16] Executive Order 13800 § 2(d), 82 Fed. Reg. 22391, 22394 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executiveorder-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[17] Letter from Senator Tom Cotton et al., U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, Dec. 20, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf; *see also* Sara Salinas, *Six top US intelligence chiefs caution against buying Huawei phones*, CNBC (Feb. 13, 2018), https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html; U.S. Senate Select Committee on Intelligence, Worldwide Threats Hearing (Feb. 13, 2018), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0.

report's recommendations that "the United States . . . view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies," and that U.S. government systems and contracts "not include Huawei or ZTE equipment."[18]

12. Responding to continuing concerns over the purchase and use of communications equipment from certain foreign entities, Congress in 2017 passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA), which, among other provisions, bars the Department of Defense from using "[t]elecommunications equipment [or] services produced . . . [or] provided by Huawei Technologies Company or ZTE Corporation" for certain critical programs, including ballistic missile defense and nuclear command, control, and communications.[19]

13. In 2018, Congress passed, and the President signed into law, the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA).[20] Section 889(b)(1) of the 2019 NDAA prohibits the head of an executive agency from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.[21] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services" as (1) telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities; (2) video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities; (3) telecommunications or video surveillance services provided by such entities or using such equipment; or (4) telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country, where "covered foreign country" is defined as the People's Republic of China.[22]

14. Multiple agencies in the Executive Branch have also initiated separately and collectively a widespread effort to protect the nation's communications networks from potential security threats. In November 2018, the Department of Homeland Security (DHS) convened the Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force), a public-private partnership formed to examine and develop consensus recommendations to identify and manage risk to the global information and communications technology supply chain.[23]

15. In December 2018, the Federal Acquisition Security Council (FASC or Council) was established pursuant to the SECURE Technology Act.[24] The Council includes representatives from the

---

[18] Letter from Senator Tom Cotton et al., U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, Dec. 20, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf; *see also* Letter from Hon. Ajit Pai, Chairman, FCC, to Senator Tom Cotton, U.S. Senate, March 20, 2018, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0323/DOC-349859A1.pdf.

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

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

[21] *See* Pub. L. 115-232, 132 Stat. 1636, 1917, Secs. 889(a)-(b)(1).

[22] *See* Pub. L. 115-232, 132 Stat. 1636, 1918, Secs. 889(f)(2)-(3). The definition is also subject to certain carve-outs. *See id.* at 1917, Secs. 889(a)(2)(A)-(B).

[23] Department of Homeland Security, Press Release, *DHS Announces ICT Supply Chain Risk Management Task Force Members* (Nov. 15, 2018), https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members.

[24] See P.L. 115-390, 132 Stat. 5173, https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf.

Office of Management and Budget (which also chairs the Council), the General Services Administration (GSA), DHS, the Office of the Director of National Intelligence (ODNI), the Department of Justice (DoJ), the Department of Defense (DoD), and the Department of Commerce (DoC).[25] The Council is tasked with developing a government-wide strategy for addressing supply chain risks from information and communications technology purchases, facilitating information sharing within the government and the private sector, and serving as the central, government-wide authority for supply chain risk mitigation activities.[26] The FASC is also responsible for establishing procedures to (1) facilitate the exclusion of entities and covered services and equipment from agency procurements, and (2) enable the removal of such services and equipment from agency information systems when it determines that those items or the parties providing them present a supply chain risk.[27] While the FASC is tasked with recommending exclusion or removal orders, the heads of DHS, DoD, and ODNI (or their delegates) have the authority to issue and rescind exclusion or removal orders for the civilian, defense, or intelligence agencies, respectively.[28] Before providing its recommendation to the heads of DHS, DoD, or ODNI, the FASC must provide the named entity with notice of the recommendation and a 30-day opportunity to respond to the recommendation. Based on FASC's recommendation and the entity's response, DHS, DoD, and ODNI officials may issue exclusion or removal orders for an entity or covered type of equipment or service.[29]

16. In February 2019, the ICT SCRM Task Force officially announced that it would focus its initial activity on: (1) developing a common framework for the bi-directional sharing of supply chain risk information between government and industry; (2) identify processes and criteria for a threat-based evaluation of information and communications technology supplies, products, and services; (3) identify market segment(s) and evaluation criteria for a Qualified Bidder and Manufacturer List(s); and (4) produce policy recommendations to incentivize the purchase of information and communications technology for original manufacturers or authorized resellers.[30]

17. On May 15, 2019, the President signed the Executive Order on Securing the Information and Communications Technology and Services Supply Chain,[31] which declares a national emergency with respect to the unrestricted acquisition or use of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries. Invoking the authority of the International Emergency Economic Powers Act and consistent with the National Emergencies Act,[32] the Executive Order prohibits

[25] See P.L. 115-390, 132 Stat. 5173, 5179, Secs. 1322(b)-(c).

[26] *See* P.L. 115-390, 132 Stat. 5173, 5180-81, Secs. 1323(a).

[27] *See* P.L. 115-390, 132 Stat. 5173, 5181, Secs. 1323(c)(1).

[28] *See* P.L. 115-390, 132 Stat. 5173, 5182, Secs. 1323(c)(5).

[29] *See* P.L. 115-390, 132 Stat. 5173, 5182-83, Secs. 1323(c)(3), (5).

[30] Department of Homeland Security, Press Release, *CISA's ICT Supply Chain Risk Management Task Force Launches Work Streams* (Feb. 26, 2019), https://www.dhs.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams. In September 2019, the ICT SCRM Task Force released an interim report detailing recommendations regarding strategic priorities and direction for future ICT SCRM Task Force efforts. *See* Department of Homeland Security, Report, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report* (Sep. 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

[31] Executive Order 13873, 84 Fed. Reg. 22689, Executive Order on Securing the Information and Communications technology and Services Supply Chain (May 15, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (Executive Order 13873).

[32] 50 U.S.C. §§ 1701-1708 (IEEPA); 50 U.S.C. ch. 34 (National Emergencies Act).

"any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States" for certain covered transactions.[33] The Executive Order applies to transactions that (1) involve information and communications technology of persons with a nexus to a "foreign adversary," and (2) pose an undue risk to U.S. telecommunications technology and infrastructure or the national security.[34] The Executive Order applies only to those transactions initiated, pending, or completed after the date of the Executive Order.[35] Pursuant to the Executive Order, the Secretary of Commerce, in consultation with other named departments, agencies, and offices within the federal government, will issue regulations consistent with the Executive Order.[36]

18. *Commission Efforts to Address Threats to National Security*. Congress created the Commission, among other reasons, "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 . . . ."[37] The FCC has therefore taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats. For example, the Spectrum Act of 2012 prohibited persons and entities who have been, for reasons of national security, barred by any federal agency from bidding on a contract, participating in an auction, or receiving a grant, from participating in auctions under the Spectrum Act.[38] Pursuant to the Spectrum Act, the Commission adopted rules prohibiting such persons from participating in spectrum auctions as well as prohibiting such persons and entities from participating in incentive auctions.[39]

19. The Commission also assesses national security, law enforcement, and foreign policy concerns in reviewing applications to transfer a spectrum license, a cable landing license, or telephone lines, among other things, when an applicant has reportable foreign ownership.[40] Our rules governing these types of reviews recognize that other federal agencies have specific expertise in these matters and that the public interest analysis would benefit from seeking the views of certain Executive Branch agencies as they relate to applicants with foreign ownership.[41] In the past, the Commission has referred certain applications to Executive Branch agencies for their expert advice when the applicant has reportable foreign ownership,[42] or where an applicant or its U.S. parent seeks to exceed the foreign

[33] Executive Order 13873 § 1(a).

[34] Executive Order 13873 § 1(a)(i)-(ii).

[35] Executive Order 13873 § 1(a).

[36] Executive Order 13873 § 2(b).

[37] 47 U.S.C. § 151.

[38] *See* 47 U.S.C. § 1404.

[39] *See* 47 CFR § 1.2105(a)(2)(xiii).

[40] *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919-21, paras. 61-66 (1997) (*Foreign Participation Order*); Order on Reconsideration, 15 FCC Rcd 18158 (2000); *see Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, Notice of Proposed Rulemaking, 31 FCC Rcd 7456, 7457, para. 4 (2016) (*Executive Branch Process Reform NPRM*).

[41] *Foreign Participation Order,* 12 FCC Rcd at 23919, 23921, paras. 61-62, 66; *see also Executive Branch Process Reform NPRM*, 31 FCC Rcd 7456, 7457, paras. 4.

[42] *Executive Branch Process Reform NPRM,* 31 FCC Rcd at 7458-59, paras. 6-7. The federal agencies include the Department of Homeland Security (DHS), the Department of Justice (DoJ, including the Federal Bureau of Investigations), the Department of Defense (DoD), the Department of State, the Department of Commerce and the National Telecommunications and Information Administration (NTIA), the United States Trade Representative, and the Office of Science and Technology Policy. *Id*. at 7458, para 8 & n.16. Of these, the national security agencies—DHS, DoJ, and DoD—are known as "Team Telecom."

ownership benchmarks of section 310(b) of the Act.[43] Upon completion of their review, these Executive Branch agencies notify the Commission of their recommendation.[44] National security and law enforcement agencies may have no comment, or may advise the Commission that they have no objection to the grant of an application so long as the Commission conditions the grant on requiring the authorization holder to comply with the terms of a relevant mitigation agreement.[45] These agencies may also recommend that the Commission deny an application based on national security or law enforcement grounds.[46]

20. In July 2018, Executive Branch agencies for the first time recommended that the Commission deny an application for international section 214 authority on national security and law enforcement grounds.[47] The application was filed by China Mobile International (USA) (China Mobile USA). In May 2019, after an extensive review of the record in that proceeding, the Commission denied China Mobile USA's application stating that it had not demonstrated that its application for authority to provide international telecommunications services was in the public interest.[48]

21. Beyond considering national security and foreign policy concerns as part of its application review process, the Commission established the Communications Security, Reliability and Interoperability Council (CSRIC), which is charged with providing recommendations to ensure the security and reliability of the nation's communications systems, including telecommunications, media, and public safety networks.[49] In 2017, the Commission chartered CSRIC VI.[50] On February 2, 2018, CSRIC VI recommended mechanisms to reduce risks to network reliability and security. These include mechanisms to best design and deploy 5G networks to mitigate risks to network reliability and security posed by, among other things, vulnerable supply chains.[51] Most recently, on March 15, 2019, the Commission chartered CSRIC VII,[52] and among its working groups are those devoted to "Managing Security Risk in the Transition to 5G," and "Managing Security Risk in Emerging 5G Implementations."[53]

22. In addition to the various steps the Commission has taken to safeguard and secure the

---

[43] 47 U.S.C. §310(b).

[44] *Id*. at 7459, para. 8.

[45] *Id*. at 7459, para. 8. Such mitigation agreements often include a requirement that applicants submit a list of principal equipment they plan to use to the agencies for approval. *See, e.g.*, Letter from Austin Schlick, President, GU Holdings, Inc., to Assistant Secretary for Border, Immigration and Trade Office of Policy, U.S. Department of Homeland Security, dated Sep. 18, 2019 (filed in SCL-LIC-20181008-00034); Letter from Nigel Bayliff, Chief Executive Officer, America Europe Connect 2 Limited, Keviv Slavadori, Director, Edge Cable Holdings USA, LLC, Austin Schlick, President, GU Holdings, Inc., and Nina Bull, VP Legal, Optibulk Havfrue AS, to Assistant Secretary for Border, Immigration and Trade Office of Policy, U.S. Department of Homeland Security, dated Sep. 2, 2019 (filed in SCL-LIC-201810080511-00010); Letter from Per Helge Svensson, CEO, Tampnet Inc. and Tampnet AS and Matthew Barket, Director, Columbo Topco Limited, to Assistant Attorney General for National Security, U.S. Department of Justice, dated Feb 13, 2019 (filed in ITC-T/C-20180824-00165 and WC Docket No. 18-25).

[46] *Executive Branch Process Reform NPRM,* 31 FCC Rcd at 7459, para. 8.

[47] Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, File No. ITC-214-20110901-00289 at 4 (filed July 2, 2018), https://go.usa.gov/xEhZ7.

[48] *China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019).

[49] *See* FCC, Communications Security, Reliability and Interoperability Council, https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0.

[50] *See* FCC, Charter of the FCC's Communications Security, Reliability, and Interoperability Council (Mar. 19, 2017), https://www.fcc.gov/files/csric-charter-2017pdf.

[51] *See* FCC, Communications Security, Reliability and Interoperability Council, CSRIC VI Working Group (continued….)

nation's telecommunications networks, one of our core missions is to make "available . . . to all the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges."[54] Since its inception, the USF has operated as one of the primary mechanisms for achieving this mission.[55] The Commission provides monetary support through four separate but complementary USF programs: (1) the high cost program, which provides support to eligible carriers that provide service to high-cost areas, thereby making voice and broadband service affordable for residents living in such regions;[56] (2) the Lifeline program, which assists eligible low income customers by helping to pay for monthly telephone and broadband charges;[57] (3) the rural health care program, which helps subsidize rates for telecommunications and broadband services to health care facilities in rural areas;[58] and (4) the E-Rate program, which provides support for broadband, internal connections, and other services to eligible schools and libraries.[59]

23. The Commission has designated the Universal Service Administrative Company (USAC) as the entity responsible for administering the universal service support programs under the Commission's oversight.[60] The Commission determines the services to be supported and the applicable funding mechanisms, and it bases these policies upon the "[u]niversal service principles" set forth in section 254(b), as well as "other principles" that we "determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with" the Act.[61]

24. In response to ongoing concerns about the integrity of the communications supply chain, the Commission released a Notice of Proposed Rulemaking on April 18, 2018, which proposed and sought comment on a rule to prohibit the use of USF funds to purchase or obtain equipment or services from any communications equipment or service providers identified as posing a national security risk to communications networks or the communications supply chain.[62] The *Protecting Against National Security Threats Notice* (*Notice*) explained that the Commission has a responsibility to ensure that the public funds in the USF are not spent on equipment or services from companies that present a risk to the

(Continued from previous page)
Descriptions at 3 (Feb. 2, 2018), https://www.fcc.gov/files/csric6wgdescriptions2-2018pdf.

[52] *See* FCC, Charter of the FCC's Communications Security, Reliability, and Interoperability Council, (Mar. 15, 2019), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-vii.

[53] *See* FCC, Communications Security, Reliability and Interoperability Council, CSRIC VII Working Group Descriptions, https://www.fcc.gov/files/csric7wgdescriptionsdocx.

[54] 47 U.S.C. § 151.

[55] *See* 47 U.S.C. § 254.

[56] *See* 47 CFR §§ 54.302-54.321.

[57] We note that the Commission has, on multiple occasions, stated that the Lifeline program supports services, not end-user equipment, with the exception of temporary support for handsets in the months following Hurricane Katrina. *Lifeline and Link Up Reform and Modernization*, Third Report and Order, Further Report and Order, and Order on Reconsideration, 31 FCC Rcd 3962, 4005-4006, para. 125 (2016) (expressly declining to provide a subsidy for consumer premises equipment); *Lifeline and Link Up; Federal-State Joint Board on Universal Service; Advancing Broadband Availability Through Digital Literacy Training*, WC Docket Nos. 11-42, 03-109, 12-23; CC Docket No. 96-45, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd at 6804, para. 348 (2012) (noting that "historically the Fund has been used for services not equipment"); *cf. Fed.-State Joint Bd. on Universal Serv. Sch. & Libraries Universal Serv. Support Mechanism Rural Health Care Support Mechanism Lifeline and Link-Up*, CC Docket Nos. 96-45, 02-6; WC Docket Nos. 02-60, 03-109, Order, 20 FCC Rcd. 16883, 16889-90, para. 13 (2005) (adopting temporary rules to include the provision of a free handset along with voice service to those directly impacted by Hurricane Katrina).

[58] *See* 47 CFR §§ 54.400-417, 54.600-54.680.

communications supply chain.[63] Both Huawei and ZTE were cited repeatedly in the *Notice* as having triggered Congressional concerns regarding the potential for supply chain vulnerability and the possible risks associated with certain foreign communications equipment providers.[64] The *Notice* sought comment on whether and how to implement the proposed prohibition,[65] what types of equipment and services to include,[66] the effective date of the rule,[67] how to deal with multiyear contracts,[68] how to identify covered companies,[69] whether to include subsidiaries, parents and affiliates of covered companies,[70] how to enforce the rule,[71] the costs and benefits of the rule,[72] and the legal authority for adopting the rule.[73] The *Notice* also sought comment on other steps the Commission should consider taking, including actions in addition to or as an alternative to restricting the use of USF support.[74]

25. On October 26, 2018, the Commission released a Public Notice seeking comment on the applicability of the 2019 NDAA to the *Protecting Against National Security Threats* rulemaking and to the USF programs the Commission oversees.[75] Specifically, the *USF National Security Public Notice* sought comment on how to interpret section 889 of the 2019 NDAA in light of this proceeding.[76]

III. REPORT AND ORDER

26. Based on our review of the extensive record in this proceeding, we adopt 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,

(Continued from previous page)

[59] *See* 47 CFR §§ 54.500-54.523.

[60] *See Changes to the Board of Directors of the National Exchange Carrier Association, Inc.; Federal-State Joint Board on Universal Service*, CC Docket Nos. 97-21, 96-45, Report and Order and Second Order on Reconsideration, 12 FCC Rcd 18400, 18415, para. 25 (1997); *see also* 47 CFR § 54.702 (establishing the USF Administrator's functions and responsibilities).

[61] 47 U.S.C. § 254(b)(7).

[62] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, 33 FCC Rcd 4058, 4058, para. 2 (2018) (*Notice*).

[63] 47 U.S.C. 254(b)(1); *Notice*, 33 FCC Rcd at 4062-63, para. 13.

[64] *See Notice*, 33 FCC Rcd at 4059-60, paras. 4-6. Huawei filed numerous comments, reply comments, and *ex partes* in this proceeding.

[65] *See Notice*, paras. 13-14.

[66] *See Notice*, paras. 15.

[67] *See Notice*, para. 17.

[68] *See Notice*, para. 18.

[69] *See Notice*, paras. 19-23.

including upgrades to existing equipment and services.[77]

27. In addition to adopting this rule, we initially designate Huawei Technologies Company and ZTE Corporation 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. Our actions today are informed by the evidence cited herein, including the actions of other agencies and branches of the government and similar assessments from other countries.

A. Spending Universal Service Funds Should Not Endanger National Security

28. As we stated in the *Notice*,[78] 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. This 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,[79] and we find it very significant that the U.S. Department of Justice (DoJ) has expressed its strong support for this conclusion.[80] We also agree 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."[81] The record persuades us 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.

29. 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*, 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.[82] As the

(Continued from previous page)

[70] *See Notice*, para. 25.

[71] *See Notice*, paras. 26-30.

[72] *See Notice*, paras. 33-34.

[73] *See Notice*, paras. 35-36.

[74] *See Notice*, para. 31.

[75] *See Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain National Defense Authorization Act for Fiscal Year 2019*, WC Docket No. 18-89, Public Notice, 33 FCC Rcd 10183, 10183, para. 1 (2018) (*USF National Security Public Notice*). In addition, on June 27, 2019, Commissioner Starks hosted a workshop in which participants, including security experts and rural wireless carrier representatives, discussed network security threats posed by insecure equipment and how to respond. Workshop participants voiced their concerns and suggestions for moving forward. "Security Vulnerabilities Within Our Communications Networks: Find it, Fix it, Fund it," *available at* https://www.fcc.gov/news-events/events/2019/06/security-threat-within-our-communications-networks-find-it-fix-it-fund-it; *see also* Letter from Caressa D. Bennet, General Counsel, Rural Wireless Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed July 1, 2019) (RWA Workshop Comments); Letter from Sarah Tyree, Vice President, CoBank, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed July 1, 2019) (CoBank Workshop Comments); Letter from Dileep Srihari, Senior Policy Counsel and Acting Head of Government Affairs, Telecommunications Industry Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed June 28, 2019); Letter from David A. LaFuria, Lukas, Lafuria, Gutierrez & Sachs LLP, Counsel for Union Telephone Company, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed June 27, 2019).

[76] *See USF National Security Public Notice* at 2.

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).[83] We adopt this rule as just such a restriction, based on our conclusion that it is critical to the provision of "quality service"[84] 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.

30. We disagree with commenters who suggest that adopting this rule violates the principle that "[q]uality services should be available at just, reasonable, and affordable rates."[85] 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.[86] Furthermore, we are 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.[87] 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, we would be shirking our responsibility to the American public if we were to ignore threats to our security posed by certain equipment manufacturers simply because that equipment was cheaper.

31. 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

(Continued from previous page)

[77] This prohibition applies to any subsidiaries and affiliates of USF recipients to the extent that such subsidiaries and affiliates use USF funds.

[78] *Notice*, 33 FCC Rcd at 4069-70, para. 36.

[79] *See China Mobile International (USA) Inc.*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3362, para. 2 & n.7 (2019); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23918-21, paras. 59-66 (1997) (*Foreign Participation Order*).

[80] *See* Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, Federal Communications Commission at 1 (Nov. 13, 2019) (DoJ Letter) ("Our national defense will depend on the security of our allies' networks as well as our own. Protecting our networks (rural and urban alike) from equipment or services offered by companies posing a threat to the integrity of those networks is therefore a vital national security goal.").

[81] TIA Comments at 68. *See also* TIA Comments at 69 ("[A] White House Report estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Even if restricting support to cyber threats via USF spending is a limited act, it will help reduce the mounting costs associated with malicious cyber intrusions.") (footnote omitted); TIA Reply Comments at 78 (commenters who argue that the rule will reduce the provision of quality services at reasonable rates are incorrect because many suppliers have been able to provide quality services at reasonable and affordable rates using other suppliers); USTelecom Comments at 16 (arguing that section 254 provides the Commission with authority to establish public interest principles, such as national security, to guide the rules it establishes for USF funding).

[82] *USF/ICC Transformation Order,* 26 FCC Rcd at 17686-87, 17695, paras. 65, 86.

[83] *In re FCC 11-161*, 753 F.3d at 1046.

[84] *See* 47 U.S.C. § 254(b)(1).

is intended."[88] 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)."[89] 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."[90] In so doing, the Commission "shall consider . . . the extent to which such telecommunications services . . . are consistent with the public interest, convenience, and necessity."[91] Again, we conclude 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.[92] Our 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).

32. 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,[93] we disagree. 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.[94] 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* and the *2016 Lifeline Order*.[95]

33. We also reject arguments that the Commission may not consider national security in assessing the public interest generally or under section 254.[96] 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 *Notice* in this proceeding,[97] 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 *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

(Continued from previous page)

[85] 47 U.S.C. § 254(b)(1); *see* CCA Comments at 17 (arguing that the rule would "drive up rates without a proportionate increase in quality").

[86] TIA Reply Comments at 78.

[87] *See* TIA Reply Comments at 62-65; *2012 HPSCI Report* at 21 ("The Chinese government often provides financial backing to industries and companies of strategic importance."); *id.* at 27-31 (discussing evidence of financial ties between the Chinese government and Huawei's operations).

[88] 47 U.S.C. § 254(e).

[89] *See Connect America Fund et al.*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 1785-86, para. 64 (2011) (*USF/ICC Transformation Order*). The Tenth Circuit affirmed this interpretation in *In re FCC 11-161*, 753 F.3d 1015, 1046- 47 (10th Cir. 2014). *See Notice*, 33 FCC Rcd at 4069, para. 35 & n.59. Some commenters argue that the Commission may rely on an additional principle only after a recommendation by the Joint Board. *See, e.g.,* Huawei Comments at 28; CCA Reply Comments at 19-20, 21. But the Commission is not here establishing a new or additional principle for universal service; rather, we are basing our new rule on the existing principle that quality services should be available at just, reasonable, and affordable rates. *See* 47 U.S.C. 254(b)(1).

[90] 47 U.S.C. § 254(c)(1).

[91] 47 U.S.C. § 254(c)(1)(D).

[92] *See* TIA Comments at 24 ("In this situation, the Commission has determined that it is in the public interest to ensure that USF dollars are not permitted to be spent on technology or services provided by companies that pose a national security risk…The Commission is therefore justified in determining that such a condition would advance the principles outlined in Section 254(b).").

bidding on a contract, participating in an auction, or receiving a grant.[98] We also have a long history of considering national security equities where other agencies have specific expertise and are positioned to make recommendations,[99] and adopting a similar process here cannot be characterized as "promot[ing] other, unrelated objectives" unrelated to the specific regulatory program at hand.[100]

34. More generally, section 201(b) of the Act authorizes this Commission to promulgate "such rules and regulations as may be necessary in the public interest to carry out the provisions of this Act."[101] 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 . . . ."[102] We conclude based on the record of this proceeding that it is necessary in the public interest to prohibit USF recipients from spending universal service funds on covered equipment or services.

35. The action we take today also implements section 105 of the Communications Assistance for Law Enforcement Act (CALEA).[103] That section requires every telecommunications carrier[104] 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. We have 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."[105] 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.[106] Telecommunications

(Continued from previous page)

[93] *See, e.g.*, CCA Reply Comments at 21 (arguing that "the FCC cannot re-define 'universal service'" under section 254(c)(1) without first "seek[ing] the Joint Board's recommendation").

[94] *See* 47 U.S.C. § 254(c)(1) ("Universal service is an evolving level of telecommunications services that the Commission shall establish periodically under this section ….").

[95] *See, e.g.*, *Modernizing the E-rate Program for Schools and Libraries*, Report and Order and Further Notice of Proposed Rulemaking, 29 FCC Rcd 8870, 8897, para. 72 & n.155 (2014) (*2014 First E-Rate Order)*; *Lifeline and Link Up Reform and Modernization*, Third Report and Order, Further Report and Order, and Order on Reconsideration, 31 FCC Rcd 3962, 3975-77, paras. 38-43 (2016) (*2016 Lifeline Order*).

[96] Huawei Comments at 27; CCA Comments at 25-26; CCA Reply at 21; RWA Reply at 17.

[97] *See Notice*, 33 FCC Rcd at 4058, paras. 1-2.

[98] *See* 47 CFR §§ 1.2105(a)(2)(xiii), 1.2204(c)(6).

[99] *See Notice*, 33 FCC Rcd at 4060-61, para. 8 (describing the interagency process for reviewing applications under section 214, under the Submarine Cable Landing License Act, and under section 310(b) when an applicant has reportable foreign ownership).

[100] Huawei Comments at 25-26.

[101] 47 U.S.C. § 201(b).

[102] 47 U.S.C. § 151.

[103] 47 U.S.C. § 1004; *see Notice*, 33 FCC Rcd at 4070, para. 36 & n.64 (asking whether there are "other statutory provisions that affect USF recipients' obligations with respect to the security of their networks" and specifically mentioning 47 U.S.C. § 1004).

carriers, including all ETCs, therefore appear to have a duty to avoid such risks.[107]

36. 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.[108] Though the rule we adopt today applies only to ETCs' use of USF funds, we disagree with Huawei's argument that the link between this obligation and the prohibition we adopt here is "remote."[109] The rule we adopt today directly implements section 105 of CALEA by reducing the likelihood that ETCs use USF funds to facilitate unauthorized surveillance. Nor does this rule require, as Huawei suggests, that we interpret 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."[110] 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 we choose here not to allow USF funds to support such use.

37. We further disagree 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.[111] The plain language of section 105 specifies not only the activation of the assistance capabilities required by section 103[112] 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.[113] We consider 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.

(Continued from previous page)

[104] The definition of "telecommunications carrier" that applies in CALEA is broader than, but inclusive of, the definition in the Communications Act. *Compare* 47 U.S.C. § 1001(8) *with* § 153(51); *see Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 14992-97, paras. 9-14 (2005) (*2005 CALEA Order*), *pet. for rev. denied*, *American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006). 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. *2005 CALEA Order*, 20 FCC Rcd at 14989, para.1.

[105] *See 2005 CALEA Order*, 20 FCC Rcd at 14993-94, para. 11 (interpreting "switching" as referring to functionality, not technology, to be consistent with the Commission's recognition that CALEA is technology-neutral). We thus disagree with CCA's argument that the security provision of CALEA is "both too narrow and too broad to justify the proposed rule." *See* CCA Reply Comments at 22.

[106] *2012 HPSCI Report* at 2-4.

[107] We disagree with Huawei that our recognition of this duty is barred by section 103(b)(1) of CALEA, 47 U.S.C. § 1002(b)(1). Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 14, 2019) at 14 (Huawei Nov. 14 *Ex Parte)*. The rule we adopt today 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.

[108] 47 U.S.C. § 229(a), (b)(1).

[109] Huawei Comments at 31-32.

[110] Huawei Nov. 14 *Ex Parte* at 15.

[111] Huawei May 14 *Ex Parte* at 5-6.

38. Congress has also determined, in section 889 of the 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.[114] We find that the goals underlying section 889 of the 2019 NDAA also support our decision to take action here. Following enactment of the 2019 NDAA, the Wireline Competition Bureau sought comment on the relevance of section 889(b)(1) to this proceeding.[115] The record now persuades us 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 our initial designation of Huawei and ZTE as such companies,[116] is consistent with section 889 of the 2019 NDAA. We agree 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."[117]

B. Companies That Pose a Threat to National Security

39. We establish a process for designating entities as national security threats for purposes of our rule. We first define "covered company" to include subsidiaries, parents and affiliates of covered companies for purposes of the rule we adopt today. In the *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.[118] Because equipment from subsidiaries, parents, and affiliates pose the same risks to network integrity as equipment directly from the covered company, we include any subsidiary, parent, or affiliate of a covered company as a covered company subject to our prohibition.

40. 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.[119] Upon the issuance of such notice, interested parties may file comments responding to the initial designation, including

(Continued from previous page)

[112] 47 U.S.C. § 1002(a) (requiring capabilities for isolation and interception of communications and for isolation and access to reasonably available call-identifying information). Section 103 does include a provision requiring those capabilities to protect the privacy and security of communications not authorized to be intercepted and to protect information regarding authorized interception. *Id.* § 1002(a)(4).

[113] *See* Communications Assistance for Law Enforcement Act and Sundry Amendments to the Code and the Communications Act of 1934, 1994 Cong. Rec. H10773-83 (Oct. 4, 1994). Significantly, the March 1994 hearing and the House Judiciary report cited by Huawei, Huawei Nov. 14 *Ex Parte* at 7-8, referred to a bill that contained the earlier language and would have been codified in Title 18 of the United States Code with no rulemaking authority for the Commission. *See also* 1994 Cong. Rec. at H10779 (Statement of Rep. Brooks) ("[T]he bill includes several provisions to improve the privacy and security in the telecommunications network.").

[114] 2019 NDAA, § 889(b)(2), 132 Stat. 1917. 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.

[115] *USF National Security Public Notice*, 33 FCC Rcd at 10183-84.

[116] 2019 NDAA § 889(f)(3) (defining "covered telecommunications equipment or services" to include "[t]elecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities)"); 2019 NDAA, § 889(b)(2), 132 Stat. 1917 ("The term 'covered foreign country' means the People's Republic of China.").

[117] TIA PN Comments (Nov. 16, 2018) at 15-16.

[118] *Notice*, 33 FCC Rcd at 4066, para. 25.

[119] This public notice shall serve as an "initial designation" of a covered company.

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 our rule. In either case, the Commission shall issue a second public notice announcing its final designation and the effective date of that final designation.[120] 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.

41. 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.[121] 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.

42. *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 our rules place on petitions for reconsideration or applications for review. If the Commission reverses its designation, the Commission shall issue an order announcing its decision along with the basis for its decision.

1. Initial Designations of Companies that Pose a Threat to National Security

43. In the *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.[122] Huawei vigorously responded to these allegations in the record of this proceeding,[123] and ZTE did not make any filings in this proceeding.

---

[120] This public notice shall serve as the "final designation" of a covered company.

[121] Because the Commission will seek to harmonize its determinations with those of other federal agencies, we find it unnecessary, as USTelecom suggests, to conduct an annual report surveying other federal agencies to determine what, if any, communications supply chain entities are designated as national security threats. *See* Letter from Mike Saperstein, Vice President, Policy & Advocacy, USTelecom, to Marlene Dortch, Secretary, FCC (filed Nov. 15, 2019) (USTelecom Nov. 15 *Ex Parte*).

[122] *See* Pub. L. 115-232, 132 Stat. 1636, 1917-18, Secs. 889(a)-(b)(1), 889(f)(2)-(3).

[123] *See* Huawei Nov. 16, 2018 Comments; Huawei June 1, 2018 Comments; Huawei Dec. 7, 2018 Reply; Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to

(continued….)

Our examination of the record re-affirms the concerns raised by the Commission in the *Notice*, and we therefore take the step of initially designating Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) as covered companies for purposes of the prohibition we adopt today.[124]

44. We agree with commenters who argue that "state actors, most notably China and Russia, have supported extensive and damaging cyberespionage efforts in the United States,"[125] and there exists a "substantial body of evidence" about the risks of certain equipment providers like Huawei and ZTE.[126] 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."[127] 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."[128] 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."[129]

45. 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.[130] 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."[131] 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.[132] And, in this 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

(Continued from previous page)
Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Oct. 11, 2019); Huawei July 2, 2018 Reply; Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Sept. 18, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed June 12, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed May 10, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Mar. 12, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Feb. 15, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Jan. 28, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Oct. 1, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 27, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 23, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 6, 2018).

[124] We conclude 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 our determinations. *See* Appendix E; s*ee also* 47 U.S.C. § 154(j) ("The Commission is authorized to withhold publication of records or proceedings containing secret information affecting the national
(continued….)

support of federal funds.[133] As explained below, we believe 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, our primary focus is on Huawei and ZTE.

46. We note, 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.[134] 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."[135] 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."[136] 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.[137] The Chinese NIL is extremely broad, applying to Chinese citizens residing outside of China.[138] Article 11 specifies that the law's powers are not limited to Chinese soil,[139] 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.[140] 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.[141] As a consequence, our primary focus in this Report and Order is on Huawei and ZTE.

(Continued from previous page)
defense."); *Use of Classified Information*, FCC 78-755, 44 RR2d 607, para. 10 (1978) (noting that classified information affecting the ultimate decision would be retained "to ensure meaningful judicial review should any disclosure be deemed necessary in a later review of these proceedings"); *Policy to Be Followed in Future Licensing of Facilities for Overseas Communications*, Docket No. 18875, Order, FCC 78-756, 69 F.C.C.2d 1232, 1232, para. 3 (1978) (noting that "the Commission is legally empowered to receive classified national defense information and to use that information as the basis for a decision"); *see also Bendix Aviation Corp. v. FCC*, 272 F.2d 533, 535-36, 538-40, 544 (D.C. Cir. 1959) (upholding reliance on undisclosed classified information to justify allocation of spectrum for government use); *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019).

[125] TIA Comments at 10.

[126] USTelecom Comments at 3 ("[T]here is a substantial body of evidence suggesting that risks to the confidentiality, integrity, and authenticity of the nation's communications networks emanate from the use of certain providers of network equipment and services, including Huawei, ZTE, and Kaspersky Labs."); s*ee also* RWR Advisory Group, Assessing Huawei Risk: How the Track Record of the CCP Should Play into the Due Diligence of Huawei's Partners and Customers, at 3-4 (May 2019), https://www.rwradvisory.com/wp-content/uploads/2019/05/Assessing-Huawei-Risk.pdf (RWR 2019 Report).

[127] NATO Cooperative Cyber Defence Centre of Excellence, "Huawei, 5G, and China as a Security Threat, at 7, 10 (2019), https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf (NATO Cyber Defence Centre Paper).

[128] RWR 2019 Report at 8.

[129] *2012 HPSCI Report* at 8.

[130] *See 2012 HPSCI Report* at 3 (observing that during product development, "malicious hardware or software [could be] implant[ed] into critical telecommunications components and systems").

2. Huawei Technologies Company

47. We initially designate Huawei Technologies Company, along with its parents, affiliates, and subsidiaries, as a covered company for purposes of our rule.

48. We find 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.[142] 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."[143] 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.[144]

49. Although Huawei argues that its affiliates in the United States are not subject to state security laws,[145] we are not persuaded to excuse these affiliates from the scope of our prohibition. One expert has noted that the nature of the Chinese system "recognizes no limits to government power."[146] Irrespective of their physical location, these affiliates still remain subject to Chinese law.[147]

50. 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

(Continued from previous page)

[131] *2012 HPSCI Report* at 3-4.

[132] *See* 2018 NDAA, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656; 2019 NDAA, 132 Stat. 1917, Sec. 889.

[133] DoJ Letter at 2.

[134] *See* Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities (2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.

[135] DoJ Letter at 2.

[136] *See* Chinese National Intelligence Law, Article 7; *see also China Mobile International (USA) Inc.*, Memorandum Opinion and Order, ITC-214-20110901-00289, 34 FCC Rcd 3361, 3370, para. 17 & n.9 (2019).

[137] *See* Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[138] *See* Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities at 3 (2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.

[139] RWR 2019 Report at 24.

[140] *See* RWR Advisory Group, A Transactional Risk Profile of Huawei at 12-13 (Feb. 13, 2018), https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf (RWR 2018 Report).

[141] *See* Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, File No. ITC-214-20110901-00289 at 4 (filed July 2, 2018), https://go.usa.gov/xEhZ7. *See also* Press Release, Office of Public Affairs, U.S. Dep't of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to

(continued….)

management of private sector companies, either formally through personnel choices, or in more subtle ways."[148] 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.[149] Ren Zhengfei exercises "ultimate veto authority over the company's material decisions."[150] Additionally, the Chinese government maintains an internal Communist Party Committee within Huawei that can exert additional influence on the company's operations and decisions.[151] 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."[152]

51. 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."[153] Huawei is reported to benefit from vast subsidies from the Chinese government, to include state-controlled financial organizations.[154] 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)."[155] 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.[156] While Huawei has refused to answer questions about its ownership and governance,[157] it can be inferred that the Chinese government clearly has a vested interest in the company's success.

52. Our actions today 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, "we are deeply concerned about

(Continued from previous page)
Steal Sensitive Military Information (Mar. 23, 2016), *available at* https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive; *see also* Press Release, Office of Public Affairs, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackerscyber-espionage-against-us-corporations-and-labor; U.S.-China Econ. and Sec. Review Comm'n, 2014 Report to Congress of the U.S.-China Economic and Security Review Commission (2014), *available at* https://www.uscc.gov/Annual Reports/2014-annual-report-congress; U.S. Dep't of Def., Annual Report to Congress: Military and Security Developments Involving the People's Republic of China (2013), *available at* http://archive.defense.gov/pubs/2013 China Report FINAL.pdf; Comm'n on the Theft of Am. Intellectual Prop., The Report of the Commission on the Theft of American Intellectual Property (May 2013), *available at* http://www.ipcommission.org/report/ip commission report 052213.pdf (IP Commission Report); Mandiant, APT1: Exposing One of China's Cyber Espionage Units (2013), *available at* https://www.fireeye.com/content/dam/fireeyewww/services/pdfs/mandiant-apt1-report.pdf (Mandiant Report); *2012 HPSCI Report*. *See also* NATO Cyber Defence Centre Paper at 11.

[142] *See* 2018 NDAA, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656; 2019 NDAA, 132 Stat. 1917, Sec. 889.

[143] U.S. Department of Commerce, Bureau of Industry and Security, Final Rule, 84 FR 22961 (May 21, 2019).

[144] *See 2012 HPSCI Report* at iv-vi.

[145] *See* Huawei Comments at 43, 87; Huawei Reply Comments at 64.

[146] Donald C. Clarke, *The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law* 3, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211; *see also id*. (noting that "the Chinese Party/state is not meaningfully restrained by Chinese law") (Clarke Report). Huawei argues that the Clarke Report does not provide support for the notion that Chinese law enforcement authorities are not constrained by Chinese laws. *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 8, 2019) *citing* Jihong Chen, "Rebuttal to Prof. Donald Clarke's Memorandum 'The Zhong Lun Declaration on the (continued….)

the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks that provides the capacity to exert pressure or control over our telecommunications infrastructure."[158] The DoJ has also stated its "strong[] support" for our action today, 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."[159]

53. In initially designating Huawei as a covered company, we also rely 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.[160] While Huawei argues that its equipment is used in other countries without undermining any nation's security,[161] several of the United States' closest allies have concluded that the risk posed by Huawei equipment and systems is too great to bear.[162] In November 2018, New Zealand's intelligence agency barred its largest telecommunications carrier, Sparc, from using Huawei equipment.[163] Likewise, in December 2018, Japan excluded Huawei from its domestic communications infrastructure.[164] Additionally, in August 2019, the Australian government announced a ban on Huawei equipment.[165] We also note that communications service providers in other countries, including BT, Orange, and Deutsche Telekom, are acting to keep Huawei equipment out of their 5G networks.[166]

54. Moreover, we are 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,[167] and that Huawei continues to make firmware updates without addressing these vulnerabilities.[168]

(Continued from previous page)
obligations of Huawei and Other Chinese Companies under Chinese Law," (Nov. 8, 2019) at 5. This argument ignores the Chinese government's authoritarian nature, lack of sufficient judicial checks, and its history of industrial espionage. *See* NATO Cyber Defence Centre Paper at 11 ("These [Chinese espionage laws] leave little assurance regarding proper judicial or public oversight to constrain the introduction of backdoors should the state deem this necessary for its broad notion of maintaining state security.").

[147] *See* Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities at 3 (2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.; *see also*, Clarke, *The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law* at 4. Huawei criticizes the Clarke Report, arguing, among other things, that Huawei is not obligated to assist in Chinese government cyberespionage activities. *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 8, 2019) *citing* Jihong Chen, "Rebuttal to Prof. Donald Clarke's Memorandum 'The Zhong Lun Declaration on the obligations of Huawei and Other Chinese Companies under Chinese Law," (Nov. 8, 2019). However, Huawei's expert concedes that his opinions "are professional opinion from the legal perspective instead of the political perspective." *Id*. at 5. As a result, his opinion does not, and cannot, address the myriad ways described herein that the Chinese government can exert influence over Chinese companies, and more specifically, has and will continue to pressure Huawei to assist with espionage activities. *See, e.g.*, *2012 HPSCI Report* at 11; TIA Reply Comments at 62-65; RWR 2019 Report at 19-21; NATO Cyber Defence Centre Paper at 8.

[148] *2012 HPSCI Report* at 11; s*ee also* TIA Reply Comments at 62-65 (discussing the large subsidies and financial benefits that Huawei and ZTE receive from state policies, including billions of dollars in credit from the Chinese Development Bank and millions in credit for Huawei and ZTE from the Export-Import Bank of China).

[149] *2012 HPSCI Report* at 13-14.

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."[169]

55. 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.[170] 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."[171] 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."[172]

56. 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."[173] This problem is compounded by Huawei's "desire to be an end-to-end provider for whole network solutions."[174] 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."[175] 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."[176] Given the multitude of evidence about the threat that Huawei

(Continued from previous page)

[150] RWR 2018 Report at 13.

[151] *2012 HPSCI Report* at 23.

[152] *2012 HPSCI Report* at 34; *see also* RWR 2018 Report at 16 (explaining that Huawei is reported to be working with other firms to enable Chinese intelligence to impair communications privacy and exploit communications networks).

[153] RWR 2018 Report at 4.

[154] RWR 2018 Report at 20.

[155] RWR 2018 Report at 20.

[156] RWR 2018 Report at 21.

[157] RWR 2018 Report at 12.

[158] *See Open Hearing on Worldwide Threats Before the SSCI*, 115th Cong., at 64-65 (Feb. 13, 2018), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#; *see also* Sara Salinas, *Six top US intelligence chiefs caution against buying Huawei phones*, CNBC (Feb. 13, 2018), https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

[159] *See* DoJ Letter at 1-2 (explaining that the DoJ is pursuing criminal charges against Huawei for, among other things, violations of the U.S. embargo on Iran, bank fraud, obstruction of justice, trade secret theft, and fraud).

[160] European Union, EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks at 26-27 (2019) (highlighting a risk scenario where a "hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities"). Huawei counters that "many other countries have not found its equipment to pose a risk," and that (continued….)

equipment presents, along with the company's unique and close relationship to the Chinese government, we disagree with Huawei's claim that there is no support for the conclusion that its equipment poses a threat.[177] 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.[178] We additionally disagree 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."[179] 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 we recognize 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.[180]

57. We also disagree with Huawei's criticisms of the Finite State report.[181] 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.[182] 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.[183] 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, we can clearly see that Huawei's security posture has not materially improved over time."[184] Indeed, we agree with Finite State that "Huawei cannot deny that, now, multiple organizations have independently found similar, substantial security vulnerabilities in their products."[185]

(Continued from previous page)
EU member states have not excluded Huawei. *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 12, 2019). As noted herein, many of our allies, including Australia, New Zealand, and Japan, have taken steps to exclude Huawei equipment from their networks. Even so, we look to our allies for their assessment of the risk posed by Huawei, but not for specific policy guidance on how to respond to this threat.

[161] Huawei Comments at 86.

[162] *See* TIA Comments at 13 (discussing that foreign governments share US security concerns regarding Huawei and ZTE).

[163] *See* Agence France-Presse, *Tech giant Huawei banned from New Zealand's 5G network over 'significant' security risks*, South China Morning Post (Nov. 28, 2018), https://www.scmp.com/news/asia/australasia/article/2175374/tech-giant-huawei-banned-new-zealands-5g-network-over; *see also* Dan Strumpf and Rachel Pannett, *New Zealand Bars Huawei From 5G*, Wall Street Journal (Nov. 28, 2018), https://www.wsj.com/articles/new-zealand-bars-huawei-from-its-5g-network-over-security-fears-1543408355.

[164] *See* Li Tao, *Japan latest country to exclude Huawei, ZTE from 5G roll-out over security concerns*, South China Morning Post (Dec. 10, 2018), https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.

[165] *See* Catherine Sbeglia, *5G in the land down under: Australia after Huawei ban,* RCR Wireless News (Sept. 20, 2019), https://www.rcrwireless.com/20190910/5g/5g-australia-huawei-ban. *See also* Stu Woo and Kate O'Keefe, *U.S. Asks Its Allies to Shun Chinese Supplier*, Wall Street Journal (Nov. 23, 2018), https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105.

[166] NATO Cyber Defence Centre Paper at 17.

58. In the light of the record in this 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,"[186] we conclude that Huawei Technologies Company, 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 we adopt today.

3. ZTE Corporation

59. We also initially designate ZTE Corporation, its parents, affiliates, and subsidiaries as a covered company for purposes of our rule.

60. As with Huawei, ZTE has close ties to the Chinese military apparatus, having originated from the Ministry of Aerospace, a government agency.[187] In fact, ZTE is still alleged to be partially owned by the Chinese government.[188] As the House Permanent Select Committee on Intelligence found, ZTE is in essence, "a hybrid serving both commercial and military needs."[189] In particular, much of ZTE's ownership constitutes state owned enterprises,[190] and, like Huawei, ZTE contains an internal Communist Party Committee, as required by the laws of China.[191] 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."[192] As described above, 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.[193]

61. 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.[194] 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.[195] The report

(Continued from previous page)

[167] Finite State, Finite State Supply Chain Assessment at 3 (2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

[168] *Id*.

[169] *Id*.

[170] U.K. Huawei Cyber Security Evaluation Center, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019 (2019) at 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf. The U.K. Oversight Board had previously noted a number of remediation activities that Huawei would need to take to mitigate significant software engineering and cyber security problems. As of the 2019 Annual Report, the Oversight Board found that Huawei's proposed remediation was "inadequate."

[171] *See id*. at 9.

[172] Intelligence and Security Committee (UK Parliament), Foreign involvement in the Critical National Infrastructure: The implications for national security at para. 19 (June 2013). https://www.parliament.uk/documents/other-committees/intelligence-security/Critical-National-Infrastructure-Report.pdf.

[173] *See* Priscilla Moriuchi, *The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture*, Recorded Future (June 10, 2019), https://www.recordedfuture.com/huawei-technology-risks/.

[174] *2012 HPSCI Rep*ort at 47 n.22.

[175] *2012 HPSCI Report* at 2.

[176] *See* Priscilla Moriuchi, *The New Cyber Insecurity: Geopolitical and Supply Chain Risks From the Huawei Monoculture*, Recorded Future (June 10, 2019), https://www.recordedfuture.com/huawei-technology-risks/.

indicated that the vulnerabilities are built into the phones during the manufacturing process and could allow malicious access to user data.[196] 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."[197] As with Huawei, ZTE's equipment has been barred in Australia and New Zealand.[198]

62. Finally, the DoJ, in supporting our 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.[199] 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.

63. Given that the Chinese government has the "means, opportunity, and motive to use telecommunications companies for malicious purposes,"[200] we conclude 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 we adopt today.

4. The Designation Process Going Forward

64. We direct the Public Safety and Homeland Security Bureau (PSHSB) to implement the next steps in the designation processes for Huawei and ZTE. We also direct 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[201]—PSHSB or the Commission shall

(Continued from previous page)

[177] *See* Huawei Reply Comments at 61-62 (citing CCA Comments at 39 for the argument that the Commission has identified "no specific evidence that Huawei or ZTE equipment and services create cybersecurity risk," and stating that companies that use Huawei equipment do not believe there are security concerns).

[178] Huawei argues that its foreign affiliates are not beholden to Chinese law. *See* Huawei May 10, 2019 *Ex Parte* at Attachment A, p. 10 (arguing that the Chinese National Intelligence Law does not foreign affiliates of Chinese companies).

[179] *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 1, 2019) *citing* Zhou Hanhua, "Expert Opinion on Article 17 of China's National Intelligence Law," (Oct. 31, 2019).

[180] Huawei also submits an expert report arguing that 5G implementation may mitigate security risks. *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov. 1, 2019). Even if this were true, it does not resolve issues related to Huawei's obligations under Chinese law, nor does it address security issues raised by equipment that is not 5G.

[181] *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Oct. 31, 2019).

[182] *Id*. at 2.

[183] *See* Finite State, Finite State Responds to Huawei Critiques, Stands by Assessment: Huawei Products Contain Significant Cybersecurity Vulnerabilities (Jul. 5, 2019), https://finitestate.io/blog/finite-state-responds-to-Huawei-Critiques-stands-by-assessment-huawei-products-contain-significant-vulnerabilities. Finite State also noted that its

(continued….)

act on such petition for reconsideration or application for review, respectively, within 120 days of the filing by a designated entity. We find 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.

65. *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 this 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.

C. Equipment and Services Covered

66. We next establish the scope of the new prohibition. The rule we adopt in this 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.

67. We find 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[202] and overseas,[203] we believe that a blanket prohibition best promotes national security, provides the most administrable rule, and eases compliance for USF recipients.[204] Given the dynamic and

(Continued from previous page)
analysis focused on "actual firmware images that Huawei distributes to its customers – more than 95% of which were the latest versions available at the time of the analysis." *Id*.

[184] *Id*.

[185] *Id*.

[186] *2012 HPSCI Report* at 2.

[187] *2012 HPSCI Report* at 38.

[188] NATO Cyber Defence Centre Paper at 9.

[189] *2012 HPSCI Report* at 38-39.

[190] *See 2012 HPSCI Report* at 39.

[191] *2012 HPSCI Report* at 40.

[192] *2012 HPSCI Report* at 44.

[193] *See* 2018 NDAA, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656; 2019 NDAA, 132 Stat. 1917, Sec. 889.

[194] *See* Phil Stewart & Jeffrey Benkoe, *Pentagon stops selling Huawei, ZTE phones in its bases, cites security*, Reuters (May 2, 2018), https://www.reuters.com/article/us-usa-china-huawei-tech/pentagon-stops-selling-huawei-zte-phones-in-its-bases-cites-security-idUSKBN1I326H.

[195] *See* Kryoptowire, *Vulnerable Out of the Box: An Evaluation of Android Carrier Devices*, at 4-7, Tbls. 1-2 (Aug. 10, 2018), https://www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf. While the USF generally does
(continued….)

wide-ranging nature of the potential threats to our networks, and our specific responsibility to protect against threats posed by USF-funded equipment and services, we find 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. We recognize 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,[205] and the rural consumers served by these providers.[206] However, we find 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.

68. Malware and vulnerabilities can be designed and built directly into communications equipment, even when that equipment is not the covered company's flagship equipment.[207] 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, we cannot allow for bad actors to circumvent our prohibitions through clever engineering.

69. We further find 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. We agree with Vermont Telephone, which argues that our rule "would eliminate uncertainty and reduce regulatory burdens that fall most heavily on small operators," and that adopting our 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."[208] Our decision to adopt a complete prohibition rather than a narrow

(Continued from previous page)
not fund end-user devices such as phones, the security concerns raised regarding ZTE mobile phones give us concerns about other ZTE equipment and services, including those funded by the USF.

[196] *See* Kryptowire, *Vulnerable Out of the Box: An Evaluation of Android Carrier Devices*, at 1 (Aug. 10, 2018), https://www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf; *see also* Kryptowire, *DEFCON 2018: Vulnerable Out of the Box – An Evaluation of Android Carrier Devices* (Aug. 10, 2018), https://www.kryptowire.com/android-firmware-defcon-2018/; Justin Lynch, *New research says ZTE phones could be hacked*, Fifth Domain (Aug. 9, 2018), https://www.fifthdomain.com/show-reporters/black-hat/2018/08/10/new-research-says-zte-phones-could-be-hacked/.

[197] Andy Keiser & Bryan Smith, The National Security Institute, Policy Paper, *Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat* at 2 (2019), https://nationalsecurity.gmu.edu/chinese-telecommunications/.

[198] Dan Strumpf and Rachel Pannett, *New Zealand Bars Huawei From 5G*, Wall Street Journal (Nov. 28, 2018), https://www.wsj.com/articles/new-zealand-bars-huawei-from-its-5g-network-over-security-fears-1543408355.

[199] *See* DoJ Letter at 1-2.

[200] *2012 HPSCI Report* at 2.

[201] 47 CFR §§ 1.106, 1.115.

[202] *See* RWA November 4, 2019 *Ex Parte* at 2.

[203] *See* TIA Comments at 48, 52; *see also* AT&T Comments at 4-5 ("By ensuring that security measures are fact-based and proportionate to legitimate security threats, U.S. policymakers would reduce the possibility of U.S.

(continued….)

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 USAC to audit and verify any such certification based on a blanket ban rather than a more selective product-by-product prohibition.

70. We are 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.[209] 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.[210] Although we understand the complications inherent in the purchasing process, we believe 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 we to find white labeling as outside the scope of our 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.[211]

(Continued from previous page)
restrictions leading to the exclusion of U.S. telecommunications and information products and services from foreign markets based on unsupported security claims, or unnecessarily depriving U.S. consumers and businesses of the benefits of global supply chains."); JAB Wireless Comments at 5; NTCA Comments at 8-9.

[204] While RWA advocates in favor of a testing program that would allow impacted carriers to submit for government approval their proposed, but mission-critical, service or maintenance plans, *see* RWA Nov. 4, 2019 *Ex Parte* at 4-5, such a framework would do little to address the potential for foreign adversaries to intentionally and maliciously access or exploit equipment within our communications networks.

[205] *See* TIA Comments at 48; RWA November 4, 2019 *Ex Parte* at 2-3 (contending that impacted companies may be forced to "spend scarce funds or go into further debt to maintain" affected networks).

[206] *See* CCIA Comments at 7 (noting that "it may be difficult for USF recipients to know from which companies they are to purchase equipment, which could have an outsized impact on smaller, rural carriers. . . .[T]o the extent that Huawei equipment is on U.S. networks, it is more likely to be found on the networks of smaller, rural carriers. Therefore, the Commission should be cognizant that a ban on certain networking equipment could actually widen the digital divide by cutting off a U.S. network provider's ability to purchase equipment or removing a source of necessary subsidies."); *see also* Huawei Reply at 68.

[207] *See 2013 GAO Supply Chain Report* at 3 (arguing that adversaries may exploit vulnerabilities in the supply chain through placing malicious code into the components of equipment that could compromise the security and resilience of networks and that such vulnerabilities can be introduced in the manufacturing, assembly and distribution processes).

[208] Letter from Dr. J. Michel Guite, Chairman and CEO, Vermont Telephone Co., Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 at 2 (filed Mar. 20, 2019) at 2 (*VTel* Mar. 20, 2019 *Ex Parte*) at 2.

71. We also make 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,[212] purchase backhaul facilities and interconnection services from third parties,[213] 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.[214] 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 our goal of securing American communications networks and incentivizing the replacement of such equipment with equipment from trusted vendors.[215]

72. We note that our 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 we caution USF recipients that choose to install new equipment or purchase new services from covered companies.

(Continued from previous page)

[209] *See, e.g.*, EchoStar Comments at 6; TIA Comments at 48. We also note that the 2019 NDAA included a carve-out that excluded products that cannot route or redirect user data traffic, or which do not provide visibility into user data. *See* Pub. L. 115-232, 132 Stat. 1636, 1917, Secs. 889(a)(2)(A)-(B). However, we find that a blanket prohibition on the use of USF funds is necessary because it increases the likelihood of preventing engineered, backdoor access to the network regardless of the types of equipment or components involved.

[210] *See Notice*, 33 FCC Rcd at 4066, para. 25; RBA Comments at 8; CCA Reply at 18.

[211] For example, the DoJ recently filed criminal charges against an American company for allegedly "selling Chinese-made equipment with known cybersecurity vulnerability to government and private customers while falsely representing that the equipment was made in the United States and concealing that the products were manufactured in the People's Republic of China." Press Release, "Aventura Technologies, Inc. and its Senior Management Charged with Fraud, Money Laundering and Illegal Importation of Equipment Manufactured in China," Department of Justice, U.S. Attorney's Office, Eastern District of New York (Nov. 7, 2019), *available at* https://www.justice.gov/usao-edny/pr/aventura-technologies-inc-and-its-senior-management-charged-fraud-money-laundering-and.

[212] *See* Letter from Caressa D. Bennet, General Counsel, Daryl A. Zakov, Assistant General Counsel, Rural Wireless Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 3 (filed Nov. 4, 2019) (RWA November 4, 2019 *Ex Parte*); Letter from Caressa D. Bennet, General Counsel, Rural Wireless Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 1 (filed Nov. 7, 2019) (RWA November 7, 2019 *Ex Parte*); Letter from Caressa D. Bennet, General Counsel, Rural Wireless Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 1 (filed Nov. 12, 2019) (RWA November 12, 2019 *Ex Parte*); Letter from David A. LaFuria, Counsel for Union Telephone Company, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Nov.8, 2019) at 3.

[213] *See* RWA November 7, 2019 *Ex Parte* at 2; RWA November 12, 2019 *Ex Parte* at 1.

[214] *See* RWA November 4, 2019 *Ex Parte* at 3. 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. *See* RWA November 4, 2019 *Ex Parte* at 3.

[215] Given these clarifications, we disagree with commenters who assert that the rule we adopt today does not provide a clear, bright line for compliance. *See, e.g.*, Union Telephone Nov. 8, 2019 *Ex Parte* at 3; RWA Nov. 12, 2019 *Ex Parte* at 2; Letter from Alexi Maltas, Senior Vice President & General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC (Nov. 13, 2019). *But see VTel* Mar. 20, 2019 *Ex Parte* at 2 (arguing that the

(continued….)

Where a project involves the purchase of such equipment, we believe 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. We are 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, we do 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 we remind recipients that such expenditures will be subject to the audit and enforcement mechanisms described herein.[216]

73. We agree with commenters who suggest a whole-of-government approach to supply chain security.[217] Our oversight of the USF requires us to act so that USF funds are not used in a manner that undermines the security of communications networks. In addition, we have 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 we adopt today applies only to equipment and services in the context of the USF, so we believe this limited application of the prohibition will advance the interests of network security and will provide necessary certainty to affected USF participants.[218] In short, our actions in this Report and Order *are* a vital part of that approach and will complement the activities of other federal agencies and Congress.[219]

74. We disagree with RWA, which contends that the prohibition we adopt today should extend only to "additional equipment" and "new services" not yet procured and deployed;[220] 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 we adopt today 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.

75. We acknowledge 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.[221] While this may be true in the case of some rural carriers, we are 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

(Continued from previous page)
rule "would eliminate uncertainty and reduce regulatory burdens that fall most heavily on small operators," and that adopting our 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.").

[216] *See* CCA Comments at 44-45; RWA Reply at 34; RWBC Reply at 36-37.

[217] *See, e.g.*, USTelecom Comments at 12-13; RWBC Reply at 35.

[218] *See* Nokia May 9, 2018 *Ex Parte* at 2 (noting that "[p]redictable criteria can also help meet the Commission's goals of securing U.S. communications networks without creating market uncertainty, or uncertainty for small USF eligible entities").

[219] *See* RWA November 4, 2019 *Ex Parte* at 6 (noting that there is bi-partisan legislation in both houses of Congress designed to assist with funding the replacement and disposal of covered equipment and urging the Commission "not to get too far ahead of Congress").

[220] RWA November 7, 2019 *Ex Parte* at 2; RWA November 12, 2019 *Ex Parte* at 2.

[221] *See* RWA November 4, 2019 *Ex Parte* at 4; *see also* Letter from Robert F. West, Executive Vice President, Infrastructure, CoBANK, to Marlene H. Dortch, Secretary, FCC (Nov. 15, 2019) at 1.

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 us to determine whether an individual provider actually could not maintain its existing network without violating our rule—and we remind 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.

76. While the rule we adopt today 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.[222] As we have already stated, the targeted rule we adopt today is part of our 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. Ours is a specific but nevertheless important role in securing the communications supply chain and our nation's communications infrastructure.

77. *Upgrades to Existing Equipment*. We next clarify that the prohibition will apply to upgrades and maintenance of existing equipment and services.[223] The rule we adopt today 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. We specifically extend 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."[224] Others argue that such upgrades should be exempted because they are necessary to preserve equipment functionality, performance, and security.[225]

78. We recognize 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. We note that such upgrades are in fact in the public interest because they would increase the security of our communications networks. Indeed, we find 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

[222] *See* RWA November 4, 2019 *Ex Parte* at 5.

[223] As explained above, 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. *See* RWA Nov. 12, 2019 *Ex Parte* at 1 (seeking clarification on whether USF funds may be used to pay third party contractors or employee salaries when those contractors or employees are maintaining or repairing equipment from covered companies).

[224] *See* NCTA Comments at 15; *see also* ITTA Comments at 6; PRTC Comments at 6-7; NTCA Comments at 9, 20, 24; USTelecom Comments at 15; RWA Reply at 38-39 ("Prohibiting the use of USF support to pay for upgrades and services would be unfairly retroactive and would destroy those reasonable investment-backed expectations."); RWBC Reply at 34-35 (arguing that "USF funds used for maintenance, software updates, and customer support should not fall within the scope of the proposed rule," and asserting that "[s]uch coverage by the rule 'would either 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'").

[225] *See* PRTC Comments at 6; *see also* NTCA Comments at 11 ("Ironically, if systems are not regularly patched, this poses a security risk by itself as out-of-date software is highly vulnerable to cyber-attack."); RWA November 4, 2019 *Ex Parte* at 2-4 (claiming that unmaintained networks are susceptible to natural disasters and threaten public safety).

communications networks of this country.[226] Further, we are 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 we may have concerns, we acknowledge 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.[227]

D. Enforcement

79. *Compliance Certifications*. We agree 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 we adopt today.[228] We direct the Wireline Competition Bureau, 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 today. Given the variety of ways that USF participants file and certify to rule compliance, we find that directing the Wireline Competition Bureau to develop such a certification for each respective program is the best means by which to implement this new certification requirement.[229]

80. *Audits and Recovery of Funds*. We believe that USAC audits are the most effective way to determine compliance with the requirements of this Report and Order, and we direct USAC to implement audit procedures for each program consistent with the rules we adopt today. 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. We note 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 we note 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.[230] To the extent that other ETCs do not yet report information to USAC that would verify compliance, we direct 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.

81. 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.[231] We see 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

---

[226] *See* AT&T Comments at 5.

[227] 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.

[228] *See, e.g.*, ALA Comments at 3-4; TIA Comments at 62; SECA Comments at 4. We do 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.

[229] Because these certifications will be subject to notice and comment during the Paperwork Reduction Act process, we see no need to issue a separate public notice seeking comment on such certifications, as USTelecom suggests. *See* USTelecom Nov. 15 *Ex Parte*.

[230] 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.

[231] *See* ALA Comments at 4; SECA Comments at 5; KSLLC Reply Comments at 10.

the service provider.[232] The determination of which entity to seek recovery from is a factual determination based on the specific facts of the violation, and we see no need to establish a rule requiring recovery only from service providers.

82. *Waivers.* We agree with commenters who support a meaningful waiver process.[233] As with any Commission rule, USF recipients may seek waivers of the rule we establish today. We disagree with commenters who suggest that we impose a 90-day shot clock for resolution of such waivers.[234] Commenters have provided no persuasive argument supporting the establishment of an arbitrary deadline for resolution of waiver requests and we similarly refrain from establishing any specialized waiver requirements for the rule adopted in this Report and Order.

E. Effective Date

83. Because of the compelling interest in protecting our national security, we conclude that the rule we adopt today 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 paragraph 79 above, including approval by the Office of Management and Budget under the Paperwork Reduction Act

84. In the April 2018 *Notice*, the Commission made clear that our proposed rule would apply only prospectively. We sought comment on how long USF recipients would need to comply with the rule and whether we should consider phasing in the rule for certain programs or USF recipients.[235] We agree with commenters who argue that the Commission should not delay the effective date of the rule.[236] 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.[237] Given the important national security concerns at stake in this proceeding, we believe it is critical that we move forward expeditiously. Moreover, because many service providers have already made the

---

[232] *See Federal-State Joint Board on Universal Service, Changes to the Board of Directors for the National Exchange Carrier Assoc., Inc., Schools and Libraries Universal Service Support Mechanism,* CC Docket Nos. 96-45, 97-21, 02-6, Order on Reconsideration and Fourth Report and Order, 19 FCC Rcd 15252 (2004) (*Fourth Report and Order*); *see Requests for Review of Decisions of the Universal Service Administrator by Hospital Networks Management, Inc.,* WC Docket No. 02-60, Order, 31 FCC Rcd 5731, 5742-43, para. 22 (2016).

[233] *See, e.g.*, TIA Reply Comments at 42; RWA Reply Comments at 37-38; RWBC Reply Comments at 37.

[234] *See* RWA Reply Comments 37-38.

[235] *See Notice*, 33 FCC Rcd at 4063-64, para. 17.

[236] *See, e.g.*, USTelecom Comments at 15; TIA Reply Comments at 17.

[237] *See* USTelecom Comments at 15 (arguing that the *Notice* and all of the numerous events taking place across the federal government have put vendors on notice and that many of its own members have chosen to buy different equipment in order to avoid security risks); *see also 2012 HPSCI Report* at iv; Letter from Senator Tom Cotton et al., U.S. Senate, to Hon. Ajit Pai, Chairman, FCC, Dec. 20, 2017, https://apps.fcc.gov/edocs_public/attachmatch/DOC-349859A2.pdf; Sara Salinas, *Six top US intelligence chiefs caution against buying Huawei phones*, CNBC (Feb. 13, 2018), https://www.cnbc.com/2018/02/13/chinashauwei-top-us-intelligence-chiefs-caution-americans-away.html; U.S. Senate Select Committee on Intelligence, Worldwide Threats Hearing (Feb. 13, 2018), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0; *Notice*, 33 FCC Rcd 4058; *USF National Security Public Notice*, 33 FCC Rcd 10183; 2018 NDAA Sec. 1656; 2019 NDAA Secs. 889(a)-(b)(1), (f)(2)-(3); Executive Order 13873 §§ 1(a), 2(b).

business decision to purchase equipment from alternative vendors in order to avoid security risks,[238] we believe 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, we do not believe that a phase-in period is necessary. Indeed, the important national security concerns at issue necessitate swift action.[239]

85. Moreover, because the rule is prospective in effect, it does not prohibit the use of existing services or equipment already deployed or in use.[240] USF recipients may continue to use equipment or services provided or produced by covered companies obtained prior to the issuance of this rule, but *may not* use USF funds to purchase, obtain, maintain, improve, modify, or otherwise support such equipment or services in any way.

86. We next clarify how our 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 we adopt will apply to all funding years that start after the designation of a covered company (so we would expect the rule prohibiting purchases from Huawei and ZTE that we initially designate today 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.[241] We believe that this 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, we direct 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 our rule.[242]

87. *Existing Multiyear Contracts*. We find that our 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 this rule. We disagree with commenters who favor such an exemption.[243] Exempting existing multiyear contracts would negate the purpose behind our rule and allow federal funds to be used to perpetuate existing security risks to communications networks and the communications supply chain.

---

[238] *See* USTelecom Comments at 15 (noting that many of its members have made the choice to "purchase the more expensive equipment in order to avoid security risks").

[239] *See* 5 U.S.C. § 553(d)(3) (stating that the required publication or service of a substantive rule shall be made not less than 30 days before its effective date, except as provided by an agency "for good cause found and published with the rule").

[240] *See* CCA Comments at 46; USTelecom Comments at 15; WTA Comments at 6; RWBC Reply at 38. We seek comment in the Further Notice on additional measures to enhance supply chain security, including requiring removal of existing equipment.

[241] *See* SECA Comments at 3; *see also* ALA Comments at 3. We note that Funding Year 2020 for both programs begins July 1, 2020.

[242] *See* USAC, *Schools and Libraries, Service Substitutions*, https://www.usac.org/sl/applicants/before-youre-done/service-substitutions.aspx (last visited Aug. 27, 2019); USAC, *Schools and Libraries, Operational SPIN Changes*, https://www.usac.org/sl/applicants/before-youre-done/spin-changes/operational-changes.aspx (last visited Aug. 27, 2019).

[243] *See, e.g.,* ALA Comments at 3; KSLLC Reply at 7; RWA Reply at 38; RWBC Reply at 37; *see also* Huawei Comments at 58 (arguing that the proposed rule would upset reliance interest to the extent it affects existing contracts); NTCA Comments at 24.

F. Constitutional Considerations

88. Some commenters raise a number of constitutional challenges to the rule we adopt here.[244] They argue that today's action 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. We find these arguments unpersuasive.

89. Both carriers and suppliers argue that a national security condition on USF funding would violate their due process rights guaranteed by the Fifth Amendment.[245] 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."[246] These due process challenges, therefore, involve two questions: First, whether carriers or suppliers are deprived of a protected interest in "property" or "liberty."[247] And second, if they are, whether the procedures employed by the Commission comport with principles of due process.[248] We conclude that the rule and its application, as adopted in this Report and Order 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. We discuss these conclusions below.

90. *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.[249] 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."[250] Because this second argument primarily concerns the due process rights of suppliers and is also raised by them in more detail, we address it—along with suppliers' other concerns—below.

91. 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."[251] Invoking *FCC v. Fox Television Stations*, CCA argues that these carriers "did not have fair notice of what would be forbidden,"[252] and invoking *General Motors Corp. v. Romein*, CCA asserts that the proposed rule "unfairly interferes with carriers' legitimate expectations without sufficient justification."[253]

---

[244] *See, e.g.*, Huawei Comments at 61-86; CCA Comments at 40-42.

[245] *See, e.g.*, Huawei Comments at 61-86; CCA Comments at 40-42.

[246] U.S. Const. amend. V.

[247] *Am. Mfrs. Mut. Ins. Co. v. Sullivan*, 526 U.S. 40, 59 (1999).

[248] *Id.*

[249] CCA Comments at 41.

[250] *Id.* at 41-42 (internal quotation omitted).

[251] *Id.* at 41.

[252] *Id.* (quoting *FCC v. Fox Television*, 567 U.S. 239, 254 (2012)).

[253] 503 U.S. 181, 191 (1992). 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. *Id.* Applying rational basis review, the Court rejected this challenge and found that the statute was a rational means of achieving a legitimate objective. *Id.* Huawei similarly argues that the rule we adopt today would violate the Administrative Procedure Act as a rule that has "unreasonable secondary retroactivity." *See* Huawei Comments at 80-81 (quoting *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 219–20 (1988) (Scalia, J., concurring)). While we acknowledge that the rule may have some retroactive effect, we find that any retroactive (continued….)

92. At the outset, at least with respect to Huawei and ZTE, we reject 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 here 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.

93. 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.[254] 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.[255] Finally, we disagree with CCA's apparent assertion that we have 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.

94. *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.[256] Assuming that a designation could result in a deprivation of a cognizable liberty or property interest, an argument which we consider and reject below, 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.[257]

95. This 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 this Report and Order. The *Notice* in this proceeding set forth Congress's concern with both companies and explained that this concern stems from the fact that both companies are subject to

(Continued from previous page)
effect is reasonable in light of the goals of this Order. Secondary retroactivity is reviewed under a reasonableness standard to determine whether or not it is arbitrary or capricious. We note 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, we conclude that multiyear contracts cannot be exempt from the rule, given that such an exemption would largely undermine the national security goals of this Order.

[254] 567 U.S. 239, 253 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

[255] *In re FCC 11-161*, 753 F.3d 1015, 1091 (10th Cir. 2014). Rejecting this argument for largely the same reasons as we do here, the court noted that "there is no basis for us to conclude that the FCC failed to give petitioners . . . adequate notice of its intent or planned regulations." *Id.*

[256] Huawei Comments at 61; CCA Comments at 41; CCA Reply Comments at 23.

[257] *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976); *see also Ralls Corp. v. Committee on Foreign Investment in the U.S.*, 758 F.3d 296, 317-18 (D.C. Cir. 2014).

such a degree of undue influence by the Chinese government as to raise counterintelligence and security concerns.[258] It was clear from the *Notice* that the Commission was considering designating them under the proposed rule. In fact, the *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,"[259] and the Wireline Competition Bureau specifically sought comment on how the 2019 NDAA should affect our approach in this proceeding.[260] Huawei responded to the *Notice* at great length,[261] and we have fully considered those arguments. As with any Commission decision, this Report and Order is subject to procedures for reconsideration by the Commission[262] and for judicial review.[263]

96. 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 this Report and Order. The initial determination adopted in this Report and Order expands on the concerns raised in the *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. We therefore conclude that Huawei and ZTE will be afforded all the process that is due in this proceeding.

97. For all other designations, the Commission will adhere to the process discussed above, 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.

98. 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.[264] There is no requirement that designations be made pursuant to the formal adjudicatory procedures of the Administrative Procedure

---

[258] *See Notice*, 33 FCC Rcd at 4059-60, paras. 4-6.

[259] *See Notice*, 33 FCC Rcd at 4065, para. 21.

[260] *USF National Security Public Notice*, 33 FCC Rcd at 10183-84.

[261] *See* Huawei Nov. 16, 2018 Comments; Huawei June 1, 2018 Comments; Huawei Dec. 7, 2018 Reply; Huawei July 2, 2018 Reply; Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Sept. 18, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed June 12, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed May 10, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Mar. 12, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Feb. 15, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Jan. 28, 2019); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Oct. 1, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 27, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 23, 2018); Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Aug. 6, 2018).

[262] 47 CFR § 1.106.

[263] 47 CFR § 1.13.

Act.[265] 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."[266] 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.[267] Additionally, Huawei and ZTE will have a further opportunity to specifically respond to their initial designation during the comment period adopted in this Report and Order.

99. Moreover, the Fifth Amendment guarantees due process only where government action threatens or deprives an individual of life, liberty, or property.[268] We find 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 we adopt today 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.[269] We find none of these arguments persuasive.

100. 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.[270] 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.[271]

101. 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."[272] 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

(Continued from previous page)

[264] Huawei Comments at 77.

[265] *See, e.g.*, *United States v. Florida East Coast Ry.*, 410 U.S. 224, 236-38 (1973); *AT&T v. FCC*, 572 F.2d 17, 21-22 (2d Cir. 1978) ("Since *United States v. Fl. East Coast Ry.*, the words 'on the record' have become, as the District of Columbia Circuit has observed, a 'touchstone test' for the applicability of the APA's trial-type procedures." (citation omitted)).

[266] *NCRI*, 251 F.3d at 148.

[267] *See Qwest Services Corp. v. FCC*, 509 F.3d 531, 536-37 (D.C. Cir. 2007) (finding nothing improper about starting a proceeding as a rulemaking and later issuing an adjudicatory decision); *see id.* ("Obviously if a party adversely affected by the adjudication argued that the switch deprived it of any right to which it would be entitled in an adjudication, we would have to assess that deprivation under conventional principles governing adjudications.").

[268] "[D]ue process is required only where government action threatens a deprivation of life, liberty, or property. . . . "[R]eputation alone, apart from some more tangible interests such as employment, is [n]either 'liberty' [n]or 'property' by itself sufficient to invoke the procedural protection of the Due Process Clause." *Orton Motor, Inc. v. United States Dep't of Health & Human Servs.*, 884 F.3d 1205, 1215 (D.C. Cir. 2018) (quoting *Paul v. Davis*, 424 U.S. 693, 701 (1976)).

[269] Huawei Comments at 61.

[270] *Cf. Greene v. McElroy*, 360 U.S. 474, 492 (1959) (finding that revocation of a security clearance "seriously affected, if not destroyed" the employee's "ability to obtain employment in the aeronautics field"); *Schware v. Board of Bar Examiners*, 353 U.S. 232, 238 (1957) (finding that due process is required before excluding a lawyer from the bar).

[271] *See* TIA Reply Comments at 92.

[272] *Trifax Corp. v. D.C.*, 314 F.3d 641, 644 (D.C. Cir. 2003).

federal funds."[273] The rule here actually does neither. It 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.[274]

102. Third, designation as a covered company does not create a deprivation by imposing a stigma sufficiently serious to alter a supplier's legal status.[275] 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."[276] 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,[277] 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.[278] 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."[279] We find that the rule adopted here does not satisfy this prong.

103. Huawei argues that the alleged stigma of a designation under the proposed rule would alter its status in two ways.[280] First, by "barring the use of universal service funds to buy the company's equipment."[281] Second, by having the practical effect of discouraging other U.S. entities from buying Huawei's equipment.[282] 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.[283] 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

---

[273] Huawei Comments at 65. Huawei argues, *inter alia*, that the proposed rule meets the definition of debarment in section 54.8 of the Commission's rules. Huawei Ex Parte at 28-29; s*ee also* 47 CFR § 54.8 (defining "debarment" as "[a]ny action taken by the Commission in accordance with these regulations to exclude a person from activities associated with or relating to the schools and libraries support mechanism, the high-cost support mechanism, the rural health care support mechanism, and the low-income support mechanism"). 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. We are similarly unconvinced by Huawei's attempt to analogize itself to a subcontractor. *See* Huawei Comments at 65 (citing *Phillips v. Mabus*, 849 F. Supp. 2d 71, 87 & n.6 (D.D.C. 2012)). 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). *See Phillips v. Spencer*, No. 11-CV-02021 (EGS), 2019 WL 3208382, at *10 (D.D.C. July 15, 2019) ("*De facto* debarment occurs when a contractor or a subcontractor has, for all practical purposes, been suspended or blacklisted from working with a government agency without due process, namely, adequate notice and a meaningful hearing.").

[274] In *Trifax*, a case on which Huawei relies, the D.C. Circuit found that plaintiff Trifax failed to show "anything remotely close to 'broad preclusion,'" pointing to the fact that the company continued to win at least some government contracts following its stigmatization by an unfavorable OIG report. *Trifax Corp. v. District of Columbia*, 314 F.3d 641, 644 (D.C. Cir. 2003).

[275] Huawei Comments at 62.

[276] *Ulrich v. City and County of San Francisco*, 308 F.3d 968, 982 (9th Cir. 2002); *Green v. Transportation Sec. Admin.*, 351 F. Supp. 2d 1119, 1129 (W.D. Wash. 2005); *Latif v. Holder*, 969 F. Supp. 2d 1293 (D. Or. 2013).

[277] In *Nat'l Council of Resistance of Iran v. Dep't of State* (*NCRI*), 251 F.3d 192 (D.C. Cir.2001), two organizations challenged the Secretary of State's designation as a "foreign terrorist organization" under AEDPA. Applying the "stigma plus" test articulated in *Paul v. Davis,* 424 U.S. 693 (1976), the Court examined whether designating an (continued….)

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.[284] Thus, we conclude that there is no cognizable deprivation of liberty or property either in adopting the rule or designating Huawei and ZTE herein this Report and Order.

104. *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."[285] 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.[286] 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."[287]

105. We disagree 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.[288] 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.[289] There is no *per se* regulatory taking under *Lucas v. South Carolina Coastal Council*,[290] 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*.[291] 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

(Continued from previous page)
entity under AEDPA would result in both stigma and a deprivation of liberty sufficient to state a due process violation. Comparing the stigma under an AEDPA designation to the stigma present in *Constantineau*, the court noted that "[r]ather than being posted as drunkards, the petitioners have been designated as foreign terrorist organizations under the AEDPA." *Id.* at 204. The stigma may also be analogous to, for example, the stigma associated with a finding that the employee of a government contractor presents "counterintelligence concerns." *Kartseva v. Department of State*, 37 F.3d 1524, 1525 (D.C. Cir. 1994). On the other hand, as TIA points out, it is unclear whether the designation will create any new stigma beyond what has already been created by the NDAA and other government actions. *See* TIA Reply Comments at 92.

[278] *See Wisconsin v. Constantineau*, 400 U.S. 433, 435 (1971) (purchasing alcohol); *Latif v. Holder*, 969 F. Supp. 2d 1293, 1304 (D. Or. 2013) (flying); *Gen. Elec. Co. v. Jackson*, 610 F.3d 110, 121 (D.C. Cir. 2010) (consideration for government contracts). For example, in *Paul v. Davis*, 424 U.S. 693, 708 (1976), the Supreme Court case establishing the so-called "stigma plus" rule, the Court examined the facts in an earlier case, *Wisconsin v. Constantineau*, 400 U.S. 433 (1971), which ruled that a law allowing for "posting"—forbidding the sale of alcoholic beverages to persons determined to have become hazards based on their "excessive drinking"—violated due process. As the Court explained in *Davis,* the law at issue in *Constantineau* went beyond mere stigma, depriving the plaintiff "of a right previously held under state law . . . to purchase or obtain liquor in common with the rest of the citizenry." 424 U.S. at 708.

[279] *See Gen. Elec. Co*., 610 F.3d at 311 (quoting *Trifax*, 314 F.3d at 644).

[280] Huawei Comments at 62-64.

[281] *Id.*

[282] *Id.*

[283] *See Miller v. Cal.*, 355 F.3d 1172, 1179 (9th Cir. 2004) (finding no "plus" because the reputational injury had not caused any actual legal disability).

[284] *See, e.g., Phillips v. Spencer*, No. 11-CV-02021 (EGS), 2019 WL 3208382, at *12 (D.D.C. July 15, 2019) ("Indeed, the D.C. Circuit has made clear that facts showing that a contractor 'won some and lost some' government (continued….)

investment-backed expectations. As explained above, 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 *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.[292] 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.

106. *Bill of Attainder.* Lastly, Huawei argues that the rule violates the Bill of Attainder Clause.[293] A law constitutes a bill of attainder "if it (1) applies with specificity, and (2) imposes punishment."[294] 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."[295] Thus, "[a] bill of attainder is a legislative act which inflicts punishment without a judicial trial."[296] Huawei argues that the rule "contravene[s] the Bill of Attainder Clause by targeting a small group of people for punitive measures."[297]

107. We find this argument unpersuasive. First, the Supreme Court has never applied the Bill of Attainder Clause to a corporation like Huawei.[298] Second, the rule cannot amount to a bill of attainder because it is not a "legislative act." We are unaware of any court opinion applying the Bill of Attainder clause to agency regulations.[299] 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.[300] Second, even if the rule were a "legislative act," it does not impose a "punishment." As this 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

(Continued from previous page)
contracting work is 'more than sufficient to preclude a reasonable jury from finding [that the contractor was] broadly precluded from government contracting . . . .'" (quoting *Trifax*, 314 F.3d at 644-45)).

[285] CCA Comments at 42 (quoting *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1015 (1992)); PRTC Comments at 7.

[286] CCA Comments at 42-44; PRTC Comments at 7.

[287] U.S. Const. amend. V.

[288] *See Connect America R&O*, 26 FCC Rcd at 17770, para. 293; *see also In re FCC 11-161*, 753 F.3d 1015, 1070 (10th Cir. 2014) (upholding the Commission's determination that companies have no "vested right to continued receipt of support at current levels" or "entitlement to ongoing USF support"); s*ee also Adak Eagle Enterprises, LLC & Windy City Cellular, LLC*, 30 FCC Rcd 5080, 5089 para. 22 (2015) ("[C]ompanies do not have a vested right to continued receipt of support at current levels, and the Commission has the discretion to balance competing universal service principles."); *Connect America Fund*, 31 FCC Rcd 8454, 8466 para. 32 (2016) ("In fact, 'there is no statutory provision or Commission rule that provides companies with a vested right to continued receipt of support at current levels, and [the Commission is] not aware of any other, independent source of law that gives particular companies an entitlement to ongoing USF support.'" (quoting *USF/ICC Transformation Order*, 26 FCC Rcd at 17771, para. 293); *In re FCC 11-161,* 753 F.3d at 1082 (holding that "the FCC reasonably interpreted § 214(e)(2) as not requiring it to offer USF support to all ETCs in a particular area"); *id*. at 1070 (upholding the Commission's determination that companies have no "vested right to continued receipt of support at current levels" or "entitlement to ongoing USF support"); *id.* at 1055, 1082 (noting that the Commission has the discretion to balance competing universal service principles); *Members of the Peanut Quota Holders Assoc. v. United States*, 421 F.3d 1323, 1335 (Fed. Cir. 2005) ("The government is free to create programs that convey benefits in the form of property, but, unless the statute itself or surrounding circumstances indicate that such conveyances are intended to be irrevocable, the government does not forfeit its right to withdraw those benefits or qualify them as it chooses.").

[289] The 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.

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]."[301]

G. Cost Benefit Analysis

108. Our cost benefit analysis focuses on the economic costs of our action.[302] We note that record evidence indicates the vast majority of such costs are attributable to ETCs receiving high-cost universal service support. We accordingly focus our 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 our action. We estimate this cost and qualitatively consider other economic costs of our action. We find these other costs to be relatively small. Given the evidence available, we estimate that the costs of today's action will not exceed $960 million and are likely to be much lower.

109. Quantifying the expected benefits of our rule is difficult. Nonetheless, we take 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.[303] 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,[304] 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

(Continued from previous page)

[290] 505 U.S. 1003 (1992).

[291] 438 U.S. 104, 124 (1978). In assessing whether such a taking has occurred, courts consider: (1) the economic impact of the regulation on the regulated party; (2) the extent to which the regulation interferes with the regulated party's reasonable investment-backed expectations; and (3) the "character" of the government action. *Id.*

[292] *See Connect America R&O*, 26 FCC Rcd at 17770, para. 293 ("Indeed, there is no statutory provision or Commission rule that provides companies with a vested right to continued receipt of support at current levels, and we are not aware of any other, independent source of law that gives particular companies an entitlement to ongoing USF support.").

[293] Huawei Comments at 78-79; Huawei Reply Comments at 59.

[294] *Foretich v. United States*, 351 F.3d 1198, 1217 (D.C. Cir. 2003) (quoting *BellSouth Corp. v. FCC*, 144 F.3d 58, 62 (D.C. Cir. 1998)).

[295] *United States v. Brown*, 381 U.S. 437, 442 (1965).

[296] *United States v. Lovett*, 328 U.S. 303, 315 (1946) (internal quotation marks omitted).

[297] Huawei Reply Comments at 59.

[298] *See Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, 909 F.3d 446, 454 (D.C. Cir. 2018) (acknowledging that the Bill of Attainder Clause's application to corporations remains an open question).

[299] *Paradissiotis v. Rubin*, 171 F.3d 983, 988–89 (5th Cir. 1999) ("No circuit court has yet held that the bill of attainder clause, U.S. Const. art. I, § 9, cl. 3, applies to regulations promulgated by an executive agency." (citing cases)).

[300] *In re FCC 11-161*, 753 F.3d 1015, 1088 (10th Cir. 2014).

[301] *See Nixon v. Administrator of General Services*, 433 U.S. 425, 473 (1977). The D.C. Circuit recently rejected a similar challenge raised by a software security company questioning a congressional ban on the federal government procuring its software, equipment, and services based on national security concerns. *See Kaspersky Lab, Inc. v.*

(continued….)

economy—is on our national communications network and how interconnected that network is and is becoming, we find it likely that any potential disruption would exceed these measures by a large margin. As a check on our analysis, consider the impact of existing malicious cyber activity on the U.S. economy: $57 billion to $109 billion in 2016.[305] 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 our 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.[306] Accordingly, if our 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 our judgment and given this analysis, we find the benefits of our 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, we note 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. We find that the benefits of safeguarding our nation against these threats alone would also significantly and substantially outweigh the costs of our rule by a large margin.

110. *Calculating the Additional Cost to Carriers*. We assume based on the initial designations that our actions today 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, we assume 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. We also estimate 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.

111. To estimate the additional cost to carriers of the prohibition and given the estimated useful lifetime of network equipment, we expect that in 10 years all Huawei and ZTE equipment that will

(Continued from previous page)
United States Dep't of Homeland Sec., 909 F.3d 446, 454 (D.C. Cir. 2018). In *Kaspersky*, the court applied a "functional test" that distinguished statutes with a punitive purpose—or punishments—from those that "reasonably can be said to further nonpunitive legislative purposes." *Id*. at 455 (quoting *Nixon*, 433 U.S. at 475).

[302] An economic cost is the extent to which resources are spent inefficiently, in this case, on more expensive suppliers.

[303] *See* Press Release, Bureau of Economic Analysis, U.S. Department of Commerce, Gross Domestic Product, Fourth Quarter and Annual 2018 (Initial Estimate) (Feb. 28, 2019), https://www.bea.gov/news/2019/initial-gross-domestic-product-4th-quarter-and-annual-2018.

[304] *See* Bureau of Economic Analysis, U.S. Department of Commerce, *Digital Economy Accounted for 6.9 Percent of GDP in 2017* (Apr. 4, 2019), https://www.bea.gov/news/blog/2019-04-04/digital-economy-accounted-69-percent-gdp-2017.

[305] *See* The Council of Economic Advisers, The Cost of Malicious Cyber Activity to the U.S. Economy at 36 (Feb. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[306] *See* Erika Harrell, Bureau of Justice Statistics, U.S. Department of Justice, Victims of Identity Theft, 2014 at 1, 6 (Sept. 2015, rev. Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

be replaced (or upgraded) with universal service support will have been replaced. At that point, the additional annual capital outlays will peak, and we generously estimate the total annual cost of our actions, including service and maintenance cost, and the required return on capital, will be between approximately $17 million and $107 million. Although we initially assume Huawei and ZTE maintain their (non-quality-adjusted) price advantage for 10 years, we then allow competition to linearly eliminate that advantage over the next ten years. On that basis, we estimate the present value of the cost this will impose on carriers to range from $160 million and $960 million.[307]

112. In developing these estimates, we first estimate the cost of replacing Huawei and ZTE equipment, and then estimate ongoing expenses. Since our Report and Order does not mandate replacement, we do not assume that all Huawei and ZTE equipment is replaced by alternative equipment. Instead, we expect that a fraction of the Huawei and ZTE equipment will be replaced. We then estimate the ongoing expenses implied by the assumed replacements. However, the sum of the estimated replacement and ongoing costs is not entirely attributable to our action. Instead, it is the difference between these costs and the costs that would have been incurred if Huawei and ZTE equipment were used. We estimate 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).

113. We estimate the average cost for a firm to replace its Huawei and ZTE equipment, excluding ongoing expenses, to range from $40 million to $45 million. We then multiply this by an estimate of the number of firms that have Huawei or ZTE equipment and rely on universal service support, and then reduce 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.

114. 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.[308] The median of the firms' replacement cost estimates is $50 million.[309] We expect that firms motivated to report their

---

[307] 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 our estimates.

[308] *See* Pine Belt Cellular Comments at 6 (noting that the "purchase price of replacement equipment for a network of Pine Belt's size would be from $6 million to $10 million"); Sagebrush Comments at 2 (estimating the cost of replacing its network at "around $57 million"); CCA Comments, Declaration of Eric J. Woody, Union Telephone Company, at 2 (estimating the purchase price of replacement equipment "to be around $40 to $45 million, with approximately another $60 to $75 million in installation costs"); CCA Comments, Declaration of Frank DiRico, NE Colorado Cellular, at 3 ("We estimate that the purchase price of replacement equipment would be in excess of $300 million including approximately $75 million to replace the core, and an additional $60 million in installation costs."); CCA Comments, Declaration of Michael Beehn, SI Wireless, at 2 ("We estimate that the purchase price of replacement equipment is $40 to $60 million."); United TelCom Reply at 2 ("United TelCom estimates that the cost of replacing all of the Huawei equipment in its network would be approximately $20 to 25 million dollars."); CCA Comments, Declaration of James Groft, James Valley Telecommunications, at 1-2 ("[James Valley Telecommunications] provides voice, mobile telephone, video, and broadband services to nearly 10,000 customers in South Dakota. . . . We estimate that the purchase price of replacement equipment is close to $5,000 per affected customer and would result in the abandonment of a network that is not fully depreciated and does not need to be replaced.").

[309] To guard against distortion due to extreme estimates, particularly given carriers' incentives to report higher estimates, we prefer 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 (continued….)

costs in the record of this proceeding have above average costs. Indeed, the reporting carriers are unlikely to be representative of carriers affected by our 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, we conservatively discount 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.

115. We generously estimate 106 firms currently buy Huawei and ZTE equipment. Huawei reports serving 85 U.S. customers in 2019.[310] 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.[311] 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, we round 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, we estimate 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.[312]

116. Lastly, we recognize capital is fungible, and carriers have some leeway to buy Huawei or ZTE equipment from other funding sources. For these carriers, we estimate they may only use universal service funds to replace between 50% and 75% of their existing Huawei or ZTE equipment.[313] 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%.

(Continued from previous page)
lowest estimate. *See* CCA Comments, Declaration of Frank Dirico, NE Colorado Cellular, at 3. 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. *See* CCA Comments, Declaration of Frank DiRico, NE Colorado Cellular, at 2-3. 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. *See* Connect America Cost Model v4.1 Default Inputs, https://www.fcc.gov/bureaus/wcb/Connect_America_Cost_Model_v4.1.1Default Inputs.zip. (For our estimates of the Report and Order costs, we use a 30% annual charge factor, as we wish to avoid understating the costs of our actions. Here, we seek to show that NE Colorado Cellular's costs are high, so we use 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). *See* CCA Comments, Declaration of Frank DiRico, NE Colorado Cellular, at 1. 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. *See* T-Mobile, *Introducing our Magenta plans*, https://www.t-mobile.com/cell-phone-plans (last visited Oct. 28, 2019).

[310] *See* Complaint for Plaintiffs at 12, para. 32, *Huawei Technologies USA, Inc. et al. v. United States et al.*, Civil No. 4:19-cv-00159 (2019), https://docs.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00159/188186/1. Alternatively, we could rely on the Dell'Oro Group's North American market share estimate for ZTE of zero. *See* Dell'Oro Group, Market Research Reports on Mobile Radio Access Network. This would imply only 85, rather than 106 purchasers, lowering our cost estimates by approximately 20%.

[311] *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. *But see* Baburajan K, telecom lead, *RAN market:*
(continued….)

117. *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. We add 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%.[314] This, with assumptions about prices discussed above, allows us to develop a cost stream associated with each year for 20 years.

118. *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 our requirement. The relevant cost of our 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).[315] The 40% estimate, which is well above the other two estimates, comes from a carrier that appears particularly concerned about our actions, and hence may have overestimated the markup. Consequently, we use 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 this Report and Order from the cost streams under the Report and Order results in a stream of cost differences. We thus estimate the present value of the cost differences for the next twenty years that would arise due to this Report and Order ranges from $160 million to $960 million.

119. *The Economic Efficiency Costs of our Actions*. So far, we have only discussed the replacement cost of our actions. To understand the potential breadth of the economic cost of our 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

(Continued from previous page)
How Huawei, Ericsson, Nokia, ZTE, Samsung performed (July 31, 2018) https://www.telecomlead.com/telecom-equipment/ran-market-how-huawei-ericsson-nokia-zte-samsung-performed-85605.

[312] *See* Jeff Johnston, Lead Economist, CoBANK Knowledge Exchange, Equipment Ban Creates Static for Rural Telecom Operators at 3, Exhibit 2 (June 2019), https://www.cobank.com/-/media/files/ked/communications/equipment-ban-creates-static-for-rural-telecom-operators-jun2019.pdf?la=en&hash=445724D786E7CFE0F169D316DADF0FA82CB0A74A.

[313] Our action 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 above. *See supra* paras. 66, 70-72.

[314] 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. *See* Connect America Cost Model v4.1 Default Inputs, https://www.fcc.gov/bureaus/wcb/Connect_America_Cost_Model_v4.1.1Default Inputs.zip.

[315] *See* MartinRoll, *Huawei – Transforming A Chinese Technology Business To A Global Brand* (Feb. 2018), https://martinroll.com/resources/articles/strategy/huawei-transforming-chinese-technology-business-global-brand/ (stating that Huawei prices itself only 5%-15% lower than its main competitors); Peter Waldman, Sheridan Prasso, and Todd Shields, Bloomberg, *Another Reason U.S. Fears Huawei: Its Gear Works and It's Cheap* (Jan. 24, 2019), https://www.bloomberg.com/news/articles/2019-01-24/huawei-stokes-u-s-fear-with-low-cost-networking-gear-that-works ("China's largest tech company makes high-quality networking gear that it sells to rural telecommunications operators for 20 percent to 30 percent less than its competitors do, says Joseph Franell, chief executive officer and general manager of Eastern Oregon Telecom in Hermiston"); CCA Comments, Declaration of James Groft, James Valley Telecommunications at 1 ("[James Valley Telecommunications] chose Huawei because it was the most cost-effective option with a 40% savings versus the 2nd most cost-effective option."). 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.

case, the cost just calculated is a key economic cost, representing an increase in resources used because our actions cause carriers to shift their purchases from more to less efficient providers. But there is a further efficiency consequence of our actions. Purchase from less efficient suppliers occurs at higher (quality-adjusted) prices.[316] 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.[317] This is true from a global as well as a domestic perspective.

120. From a global perspective, our estimate of the economic cost of our 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, our 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 our actions would be lower.

121. We reject Huawei's claims that our 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.[318] It is unlikely our 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.[319] Given this, and Aron's claim that there are high costs associated with switching from one equipment manufacturer to another, it is implausible that our actions

---

[316] If the quality-adjusted prices of Huawei and ZTE are equal to their rivals' prices, then our 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.

[317] 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. *See, e.g.*, Luis M.B. Cabral, Introduction to Industrial Organization, 16, 26 (2d ed. 2017). The reimbursement cost, ΔP*Q, swamps the distortion cost, ΔP*ΔQ, since Q is generally considerably larger than ΔQ. Thus, if higher prices reduce demand by 5% (= ΔQ/Q), then the distortion cost could not add more than 5% to the cost to the Universal Service Fund (ΔP*ΔQ/ΔP*Q = 5%).

[318] *See* Letter from Andrew D. Lipman, Counsel, Huawei Technologies Co., Ltd. and Huawei Technologies, USA, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89 (filed Oct. 11, 2019), Att. 1, p.7, 69, 85 (Expert Report of Dr. Debra J. Aron).

[319] *See,* Diane Bartz, Liana B. Baker, & Greg Roumeliotis, *Exclusive: T-Mobile, Sprint see Huawei shun clinching U.S. deal – sources*, Reuters Business News (Dec. 14 2018), https://www.reuters.com/article/us-sprint-corp-m-a-t-mobile-huawei-exclu/exclusive-t-mobile-sprint-see-huawei-shun-clinching-u-s-deal-sources-idUSKBN1OD2HO ("Like all major U.S. wireless carriers, T-Mobile and Sprint do not use Huawei equipment, but their majority owners, Germany's Deutsche Telekom AG and Japan's SoftBank Group Ltd, respectively, use some Huawei gear in overseas markets."); Juan Pedro Tomás, *US officials not explaining why Huawei poses a security risk: AT&T CEO*, (continued….)

will affect these carriers' 5G deployment plans.[320] More broadly, we find it unlikely that our 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 our rule will have "virtually no" impact on 5G deployment.[321] What is more, we find that ensuring a robust ecosystem of trusted vendors for 5G equipment (one collateral consequence of our 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.

IV. FURTHER NOTICE OF PROPOSED RULEMAKING

122. Today's Report and Order marks an important step towards securing our nation's telecommunications networks and supply chains from national security threats. At the same time, we recognize that further steps are needed to secure our communications networks. As such, we propose to require as a condition on the receipt of any USF support that ETCs not use or agree to not use within a designated period of time, communications equipment or services from covered companies. In addition to conditioning future USF support, we propose to require ETCs receiving USF support to remove and replace covered equipment and services from their network operations. To mitigate the impact on affected entities, and in particular small, rural entities, we propose to establish a reimbursement program to offset reasonable transition costs.[322] We propose to make the requirement to remove covered equipment and services by ETCs contingent on the availability of a funded reimbursement program. We appreciate that many small and rural carriers affected by today's Report and Order are already committed to securing the integrity of their networks,[323] and we expect these proposals would facilitate the transition of their equipment and services to safer and more secure alternatives and seek comment on these proposals.

123. We believe sections 201(b) and 254 of the Act provide legal authority for these proposals.[324] Section 201(b) authorizes the Commission to "prescribe such rules as may be necessary in the public interest to carry out the provisions of the Act."[325] Section 254(b) further requires the Commission to base its universal service policies on the principles of providing "[q]uality services . . . at just, reasonable, and affordable rates," as well as promoting "[a]ccess to advanced telecommunications

(Continued from previous page)
RCR Wireless News (Mar. 23, 2019), https://www.rcrwireless.com/20190322/5g/us-officials-not-explaining-shy-huawei-poses-security-risk-att-ceo (AT&T CEO Randall Stephenson reported as saying, "we are not using equipment from Chinese manufacturers."); Jessica Bursztynsky, *Verizon CEO: We're doing just fine without using any equipment from Chinese tech giant Huawei* (July 11, 2019), https://www.cnbc.com/2019/07/11/ceo-hans-vestberg-says-verizon-does-not-use-any-huawei-equipment.html.

[320] *See, e.g.,* Barclay's *Special Report 5 June 2019 5G Leadership* at 3. ("We expect the pace of 5G deployment in the US to remain largely unaffected by the restrictions, as none of the major wireless operators uses Huawei equipment.")

[321] *See* Dan Strumpf and Eva Dou, Huawei Founder Says Chinese Giant Doesn't Need the U.S., Wall Street Journal, 6 November 2019, https://www.wsj.com/articles/huawei-founder-says-chinese-giant-doesnt-need-the-u-s-11573042649.

[322] *See, e.g.*, News Release, FCC, Workshop on "Security Vulnerabilities within Our Communications Networks: Find It, Fix It, Fund It" (June 21, 2019), https://docs.fcc.gov/public/attachments/DOC-358107A1.pdf.

[323] *See, e.g.*, Letter from Alexi Maltas, Senior Vice President and General Counsel, Competitive Carriers Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, at 1 (filed Nov. 13, 2019).

[324] 47 U.S.C. §§ 201(b), 254(b).

[325] *Id*. § 201(b).

and information services . . . in all regions of the Nation."[326] As the Tenth Circuit has explained, "nothing in the statute limits the FCC's authority to place conditions . . . on the use of USF funds" that advance the purposes of the universal service programs.[327]

124. Ensuring the safety, reliability, and security of the nation's communications networks is vital not only to fulfilling the purpose of the Act but to furthering the public interest and the provision of quality services nationwide. The continued use of equipment or services produced or provided by an entity that poses a national security threat runs counter to these objectives and threatens the safety, reliability, and security of the nation's critical infrastructure. Conditioning receipt of future USF funding on not using covered equipment and services and requiring the removal and replacement of covered equipment and services will incentivize ETCs to eliminate the security shortcomings potentially present in their current operations.

125. We also believe these proposals are consistent with Congress's direction, under the 2019 NDAA, to "prioritize available funding and technical support to assist affected . . . entities to transition from covered communications equipment [as defined by the statute], and to ensure that communications service to users and customers is sustained."[328] Section 889(b)(1) read in conjunction with section 889(b)(2) further evidences the intent of Congress to limit the use of Federal funding for the acquisition of covered equipment and services by funding recipients and to incentivize the replacement of covered equipment.[329] Section 889(b)(2) specifically directs executive agencies, including the Federal Communications Commission, to prioritize available funding and technical support to assist "as is reasonably necessary" businesses, institutions and organizations in transitioning from covered to replacement equipment as a result of the implementation of the prohibition on covered equipment as set forth in section 889(b)(1).[330] The relevant legislative history "stress[es] the importance of assisting rural communications service providers, anchor institutions, and public safety organizations in replacing covered equipment and associated support services contracts as soon as practicable."[331]

126. We tentatively conclude that these statutory provisions collectively support the rules proposed herein and seek comment on this position. We also believe they are consistent with Congress's purpose in creating the agency, in part, for "the national defense."[332] We further ask commenters to identify additional, alternative sources of statutory authority that would support these proposals.

A. Removing Equipment and Services from Covered Companies

127. *Covered Companies*. We propose to have the removal and replacement requirement apply to the equipment and services produced or provided by companies designated by the Commission as posing a national security threat pursuant to the process identified in the Report and Order. We seek comment on this proposal. We also seek comment on potential alternatives.

128. *USF Recipients Subject to Requirement and Reimbursement Eligibility.* We propose to

---

[326] *Id*. § 254(b).

[327] *In re FCC 11-161*, 753 F.3d at 1046.

[328] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[329] *2019 NDAA*, Secs. 889(b)(1), (b)(2), 132 Stat. at 1917. We recognize the USF program is not a loan or grant program *per se* but interpret Congress as intending section 889(b)(1) read in conjunction with section 889(b)(2) as more broadly covering programs like USF that issue funding commitments. Failing to include USF, with annual expenditures of about $8.3 billion for the acquisition and use of communications equipment and services, would seriously undermine the purpose of section 889 of the *2019 NDAA*.

[330] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[331] H. Rep. No. 115-874 at 919 (2018) (Conf. Rep.).

[332] 47 U.S.C. § 151.

limit the removal and replacement requirement to ETCs. The covered companies initially designated in the Report and Order, Huawei and ZTE, supply equipment and services for fixed and mobile communications networks, cloud-based network solutions, and consumer devices, including Wi-Fi routers, data cards, and smartphones.[333] While these products and services are not limited to use by ETCs, we find, given our legal authority is tied to our administration of the USF, the potential replacement burden and available reimbursement funding needed, and the evidence in the record that the primary USF recipients that currently rely on Huawei and ZTE are ETCs, that the Commission should focus on the networks of ETCs, where there is the greatest concern regarding equipment and services posing a national security threat. Accordingly, we do not propose to subject other USF recipients, like rural health care providers or schools and libraries, to the prohibition on the receipt of USF funds nor to the removal and replacement requirement. We seek comment on this approach. How should we address service providers that are not currently ETCs? Should our proposed prohibition and removal and replacement requirements apply to those carriers that are designated ETCs in the future? If so, how? And should we allow otherwise qualifying carriers to become ETCs for the sole purpose of participating in any removal and replacement fund? Would such ETC designation be necessary if, for example, Congress appropriated funds for a reimbursement program that was not tied to the Fund?

129. We propose making entities subject to the prohibition and removal requirement eligible for any replacement cost reimbursement program. In addition, we seek comment on whether other "businesses, institutions, and organizations" affected by section 889(b)(1)'s prohibitions should also be able to seek available funding or technical assistance from the Commission, even if they do not participate in any of the four universal service programs. Section 889(b)(1) states that executive agencies may not "obligate or expend loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems" "that use[] covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."[334] In particular, the Conference Report's note accompanying the 2019 NDAA discusses providing assistance to "rural communications service providers, anchor institutions, and public safety organizations."[335] If we provide cost reimbursement through a USF mechanism and include entities that are not current USF recipients, we propose that any new entities would need to be eligible under existing USF requirements, such as being willing (and eligible) to be designated an ETC by the relevant commission for at least one year after first receiving funding.[336] We seek comment on this proposal. Are there any other limits we should use for defining or identifying such an affected entity?

130. We believe that ETCs are the most likely to rely on USF-supported prohibited equipment and that the potential burden and available funding needed to cover all non-ETC USF recipients may be quite high. At the same time, we recognize that limiting our proposed removal and replacement requirement to ETCs runs some risk that non-ETC USF recipients may keep otherwise prohibited equipment in USF-supported networks. Recognizing our need to balance risks and benefits, we seek comment on whether to expand our proposed removal and replacement requirement to all USF recipients, rather than limit it to only ETCs. That is, should the Commission expand this proposed requirement to any entity receiving universal service support?

---

[333] *See, e.g.*, Huawei Investment and Holding Co., Ltd., 2018 Annual Report, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh; ZTE, https://www.zte.com.cn/global/products (last visited Oct. 8, 2019).

[334] *2019 NDAA*, Sec. 889(a), (b), 132 Stat. at 1917.

[335] Conf. Rep. at 918-919.

[336] A provider must be designated as an ETC to receive high-cost support. 47 U.S.C. § 214(e)(2), (7). Similarly, there are restrictions on eligibility of schools, libraries, and rural health care facilities for the E-Rate and Rural Health Care programs. *See* 47 CFR §§ 54.501, 54.601.

131. Or should the Commission go further and prohibit the use of equipment or services from covered companies in communications networks more broadly? We seek comment on whether the Commission can and should prohibit any communications company from purchasing, obtaining, maintaining, improving, modifying, or otherwise supporting 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, regardless of whether they use universal service support to do so. If so, what penalties would apply to non-USF recipients for non-compliance? We also seek comment on whether the Commission can and should similarly expand the proposed removal and replacement requirement to non-USF recipients. What adjustments would we need to make to our proposed requirement to implement such an expansion? For example, should we also include such companies in a reimbursement program and how would this affect the burden and availability of reimbursement funding needed? Alternatively, should we allow non-USF recipients to voluntarily participate in a reimbursement program, and if so, could we do so absent legislation? Should we also require non-USF recipients to comply with an information collection similar to the one we adopt today for ETCs, and if so, could we do so absent legislation? And what would be our source of legal authority for applying a prohibition on covered equipment and services and our proposed removal and replacement requirement to non-USF recipients absent new congressional legislation?

132. Would CALEA be one potential source of such authority, and if so, what providers would be covered and how would we need to adjust a prohibition on covered equipment and services and our proposed removal and replacement requirement to account for reliance on that authority?[337] For example, in 2005, the Commission interpreted the scope of CALEA to also include facilities-based ISPs and interconnected VoIP service providers.[338] How should the Commission consider these kinds of entities with respect to a prohibition on covered equipment and services and a removal and replacement requirement?

133. *Equipment and Services Requiring Removal and Replacement.* In the Report and Order, we determined a blanket prohibition on USF funding for all equipment and services from covered companies posing a national security risk was easier to administer and would provide more regulatory certainty for USF recipients than a narrower prohibition aimed at specific types of equipment and services. The prohibition includes not only finished products by a covered company but also products containing specific components or sub-parts produced or provided by a covered company. We propose to use the same scope to identify equipment and services subject to a removal and replacement requirement. We seek comment on this proposal.

134. Including all equipment and services from covered companies creates a bright line for ETCs to make determinations for removal and replacement. This approach would also include equipment and services covered by the 2019 NDAA, which has a narrower scope, covering equipment and services that are either a "substantial or essential component of any system, or as critical technology as part of any system."[339] Section 889(b)(3) of the 2019 NDAA also excludes from its definition of covered telecommunications equipment any equipment "that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles."[340] Although we recognize using the 2019 NDAA definition would limit the replacement burden, a broader requirement increases the likelihood of preventing engineered, backdoor access to the network and should be easier for ETCs to implement and for the Commission to enforce. We seek comment on this proposal

[337] 47 U.S.C. § 229(a). For example, how would section 103(b)(1) of CALEA apply—if at all—if we were to expand our rules beyond the expenditure of federal funds? *See* 47 U.S.C. § 1002(b)(1).

[338] *Communications Assistance for Law Enforcement Act and Broadband Access and Services,* First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989 (2005).

[339] *2019 NDAA*, Sec. 889(a)(1)(A), 132 Stat. at 1917.

[340] *2019 NDAA*, Sec. 889(b)(3)(B), 132 Stat. at 1917.

and the benefits and costs of a broader requirement.

135. In the accompanying Order, we prohibit the use of universal service funds to purchase or obtain any equipment or services produced or provided by a covered company. As the FCC has recognized on multiple occasions, the Lifeline program supports services, not end-user equipment. However, some carriers participating in the Lifeline program offer free handsets to eligible consumers as part of their offering. Carriers' websites further indicate that some Lifeline ETCs offer free handsets that are manufactured by the covered companies. We seek comment on whether the distribution of such handsets to Lifeline-eligible consumers poses a risk to the integrity of Lifeline consumers' communications.

136. Alternatively, if the Commission relies on the 2019 NDAA as a source of authority for these proposed actions, should we then tailor the removal and replacement requirement to more closely adhere to the scope of equipment and services identified in the 2019 NDAA? Would limiting replacement to the equipment and services covered by the 2019 NDAA affect the estimated cost in a meaningful way? In light of the burdens that replacing existing network equipment will impose on carriers receiving USF support, how should we clearly define and identify this type of equipment in order to assist applicants and potential auditors in determining how to comply with the proposed rule?[341] Should the Commission use or reference any definitions developed by the Executive Branch for purposes of federal procurement compliance with the 2019 NDAA? Instead, should the Commission or USAC develop a list of equipment and services that must be removed and replaced? Should we specifically limit the removal and replacement to only covered equipment and services embedded or deployed in an ETC's network? To what extent should the requirement apply to the networks of ETC affiliates?

137. *Eligible Replacement Costs.* We propose to make available reasonable replacement costs for the equipment and services produced or provided by covered companies, and we seek comment on this proposal. We also seek comment on what costs associated with replacing such equipment and services are reasonable and what types of restrictions to place on equipment and service replacement costs in order to manage limited USF resources effectively and guard against waste, fraud, and abuse. How should we determine the reasonableness of the costs to replace the covered equipment or services? Should USF recipients be allowed to seek reimbursement for technology upgrades to their networks while transitioning from covered equipment and services to replacement equipment and services? To best target available funds, should the Commission prioritize payments for the replacement of certain equipment and services that are identified as posing the greatest risk to the security of networks, and what categories of equipment and services should that prioritization include? If so, how should the Commission prioritize such funds? What additional administrative burdens would such prioritization require and what impact would it have on how quickly we could remove all problematic equipment and services from our communications networks?

138. The Commission has made significant strides towards closing the digital divide and encouraging the deployment of the next generation of equipment and services. Would our proposal require ETCs replacing equipment and services to replicate the functionality of that equipment, even if the equipment or services is outdated? Could requiring the replacement of aging equipment that endangers our national security aid our efforts to close the digital divide and encourage the migration to 5G technology in rural America? We recognize the practicality that USF recipients, such as wireless carriers using older technologies, like 3G equipment, may not be able to find functionally-equivalent equipment available in the marketplace. We seek comment on how to encourage both the goal of closing the digital divide and the need to prevent wasteful spending on outdated equipment while reducing the national security risks in our Nation's networks operated and used by ETCs.

[341] *See, e.g.*, TIA Public Notice Comments, WC Docket No. 18-89, at 19-20 (filed Nov. 16, 2018) (proposing definition for covered telecommunications products); USTelecom Public Notice Comments, WC Docket No. 18-89, at 6 (filed Nov. 16, 2018) (encouraging the Commission to use the 2019 NDAA limitations on covered equipment and services).

139. As discussed in the Report and Order, some parties allege that they purchased equipment from covered companies because of significant price savings compared to equipment from other vendors.[342] We seek comment on this claim and, to the extent it is accurate, what the Commission and the private sector can do to address it. Are there measures that non-covered companies can undertake to offer lower prices to carriers seeking to replace their insecure equipment? Can carriers create joint purchasing programs to reduce their equipment costs? To what extent are the security problems discussed in this proceeding related to the lack of U.S.-based equipment vendors? Are there U.S.-supplied alternatives or replacements for products from the covered companies?[343] Finally, we seek comment on ways the Commission can ensure that, going forward, ETCs obtain and rely on equipment only from trusted vendors.

140. During the Commission's broadcast incentive auction, the Commission developed a standard to reimburse costs reasonably incurred by an entity in order to relocate or otherwise modify its facility, using a comparable facilities reimbursement standard for all eligible entities.[344] In that proceeding, the Commission decided to not provide reimbursement for new, optional features that are not already present in the equipment being replaced, but because some stations may not have been able to replace older, legacy equipment in the marketplace, the Commission would reimburse for some equipment that includes improved functionality.[345] Should we adopt a similar comparability standard for replacement costs here? Should we allow reimbursement for non-comparable equipment or services that are safer or more secure than the replaced equipment or services due to enhanced safety features, more robust encryption, more frequent security updates, and so forth? What are the cost implications of allowing covered equipment or services to be replaced with upgraded technologies and what limits or standards should we place on these upgrades? Are there efficient ways to develop estimates of replacement costs that could provide guidance to USF recipients required to make these replacements? If we do elect to allow USF recipients to upgrade their equipment and receive reimbursement, what type of showing should we require them to make to support their reimbursement requests for eligible replacement costs? We also seek comment on whether the Commission's Wireline Competition Bureau or USAC should be responsible for reviewing and acting on reimbursement requests.

141. We also seek comment on any other issues surrounding the cost to comply with our proposed rule of requiring replacement of covered equipment and services by ETCs. For instance, should the Commission adopt a cut-off date for equipment and services eligible for reimbursement as currently being considered in the United States 5G Leadership Act of 2019?[346] Should equipment and services replaced after the effective date of today's Report and Order but before the availability of a reimbursement program be eligible for reimbursement? Should we require equipment to be retired and

---

[342] *See* RWA Workshop Comments, "Statement of John Nettles, President, Pine Belt Communications" at 2; CoBank Workshop Comments, "Equipment Ban Creates Static for Rural Telecom Operators" at 2.

[343] *See, e.g.*, O-RAN Alliance, https://www.o-ran.org/ (last visited Nov. 13, 2019); News Release, FCC, Workshop on "Security Vulnerabilities within our Communications Networks: Find It, Fix It, Fund It" (June 21, 2019), https://docs.fcc.gov/public/attachments/DOC-358107A1.pdf.

[344] The Commission's spectrum incentive auction incentivized incumbent broadcast television licensees to relinquish or relocate from their bands for the repurposing and re-licensing of the spectrum via auction for, among other things, commercial mobile use. As part of that process, the Commission established a reimbursement program to compensate relocated broadcasters for costs "reasonably incurred" in relocating to new channels assigned in the repacking process. *See Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, Report and Order, 29 FCC Rcd 6567, 6812, 6820-25, paras. 598, 620-30 (2014), *aff'd, Nat'l Ass'n of Broadcasters v. FCC*, 789 F.3d 165 (D.C. Cir. 2015) (*Incentive Auction R&O*); *LPTV, TV Translator, and FM Broadcast Station Reimbursement*, *Expanding the Economic and Innovation Opportunities of Spectrum Through Incentive Auctions*, MB Docket No. 18-214, GN Docket No. 12-268, Report and Order, 34 FCC Rcd 1690 (2019).

[345] *See id.*

[346] *See* S. 1625, 116th Cong. (2019).

scrapped? To provide good incentives for carriers in selling scrapped equipment, should we allow them to keep some fraction, e.g., one third of the sale value? How should we also factor in associated business costs, such as existing loans or sped-up depreciation?[347] Using the Commission's broadcast incentive auction for comparison, lost revenues were not eligible for reimbursement due to a statutory prohibition. We propose to make lost revenues ineligible for reimbursement due to the difficulty in administration and seek comment on this approach.

142. We also seek comment on the necessity of requiring replacement of certain equipment and services. Requiring such replacement in instances where replacement is unnecessary is a waste of public funds and contrary to our goals for the USF programs. We seek comment on whether to narrow our proposed rule to require that ETCs remove, but not replace, covered equipment and services. Are there scenarios in which replacement of removed equipment and services is not necessary? Are there networks in which there is sufficient redundancy that the removal of covered equipment and services need not be replaced? Are there other reasons why ETCs may not need to replace removed equipment and services?

143. *Available Funding*. We propose to seek an appropriation or authorization of funds from Congress to fund our proposed reimbursement program and to provide support for replacing existing equipment and services posing a national security threat in USF-supported networks. Given the potential national security risks in leaving existing equipment in USF-funded networks, as well as Congress' direction to the Commission to "ensure that communications service to users and customers is sustained,"[348] we believe Congress will want to play a role in providing financial resources to resolve a time-limited issue. For example, on May 22, 2019, Senators Cotton, Markey, Warner, and Wicker introduced S. 1625, the United States 5G Leadership Act of 2019, which would establish a $700 million Supply Chain Security Trust Fund using auction proceeds to replace equipment or services that are determined by the Commission to pose a national security risk.[349] We seek comment on our proposal, and on the appropriate level of funding the Commission should request from Congress.

144. Alternatively, if Congress does not appropriate funding for the Commission, we seek comment on using USF funding to provide support for replacing existing equipment and services posing a national security threat in the networks used by USF recipients. As noted in the record, there are existing budgets or caps for all four universal service programs.[350] Should we account for replacement reimbursement costs from the USF under the cap or budget for the USF program that funded the equipment in the first place? How would using USF support affect the contribution factor? Should we consider establishing a new, time-limited USF program for this purpose? If we do not establish new USF replacement disbursement program, we seek comment on whether there is a way to prioritize existing USF support using the existing programs. For instance, should we consider advance funding for affected entities under the high cost support programs? Or, are there specific Commission rules that we could change or waive, such as the E-Rate program's category two budget limits or equipment transfer rules for schools and libraries that may need to replace existing equipment or services?[351] Within the confines of the USF program, what level of support is appropriate for funding these replacement costs?

---

[347] *See, e.g.*, CCA et al Reply Comments at 14; RBA Comments at 14.

[348] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[349] *See* United States 5G Leadership Act of 2019, S. 1625, 116th Cong. (2019).

[350] *See* ITTA Public Notice Comments, WC Docket No. 18-89, at 7-8 (filed Nov. 16, 2018) (arguing that existing program budgets are already set and forcing ratepayers to fund replacement costs "would be tantamount to an unfunded mandate").

[351] *See* 47 CFR §§ 54.502(b) (establishing a five-year budget for schools and libraries requesting funding for internal connections, managed internal broadband services, and basic maintenance of internal connections); 54.513(b) (setting rules for disposal of equipment).

145. What are the total costs of removing and replacing equipment and services from covered companies as proposed? For instance, TIA provides an estimate of less than 1,500 cell sites costing approximately $150 million plus installation.[352] At the other end of the cost estimates, one declaration stated that it could cost $410 million for a single carrier to transition the equipment out of its network.[353] RWA states that approximately 25% of its members have deployed either Huawei or ZTE in their networks, with estimated costs of $800 million to $1 billion in costs to replace equipment before the end of its lifespan and depreciation for those 12 to 13 companies.[354] They also cite information from Huawei, who is an associate member of RWA, that it has 40 wireless and wireline customers in the United States, whose additional costs beyond its membership RWA could not estimate.[355] How accurate are these estimates? What other sources of information are available to estimate the total cost that would be needed for our proposed reimbursement program? (Below, we adopt an information collection to aid our inquiry).

146. Finally, should we cap the amount of funding available to these affected entities? If we set such a cap, we seek comment on ways to prioritize the limited funding if the replacement funding amount sought exceeds the total available funds. Should the Commission separately cap the amount eligible for each individual funding request? Section 889(b)(2) states that the Commission shall "prioritize available funding . . ." that is "reasonably necessary for those affected entities to transition."[356] As in the United States 5G Leadership Act, should we limit eligibility for assistance based on the maximum number of customers that an affected entity serves?[357] Would such a limitation ensure that the limited funds are properly targeted to those entities with the most need? How should the Commission interpret "reasonably necessary"?[358] Should we require affected entities to contribute some portion of the funding to replace the covered equipment and services, i.e., what portion, if any, of an entity's replacement cost should be borne by the requesting entity? If so, what percentage is appropriate to limit waste by incentivizing cost-efficient decision-making by ETCs, while ensuring entities can continue to serve their customers, patrons, and patients?

147. *Preventing Waste, Fraud, and Abuse.* As we propose to prohibit ETCs from using equipment and services from covered companies, we propose to add a certification to existing program forms. USF recipients would need to certify they are complying with the proposed rule(s), either by certifying that they do not have covered equipment and services or that they are working to replace covered equipment and services with the funding received. We propose requiring a duly authorized individual from the entity under penalty of perjury sign the certification. Are there any concerns with this certification requirement? Do all USF participants have, or can they obtain through reasonable due diligence, sufficient insight into their equipment and services to make these certifications? Are there any other enforcement mechanisms that we should consider?

148. We also propose to require all affected entities that receive funding to replace equipment or services to file annual certifications of compliance that all support will be used for its intended purpose.[359] This is consistent with section 254 of the Act, which requires that USF recipients "shall use

[352] *See* TIA Reply Comments at 30-31 (estimating costs to replace equipment at a single site to be $100,000, but excluding core network equipment).

[353] *See, e.g.*, CCA Comments, DiRico Decl. at 3.

[354] *See* Letter from Caressa D. Bennet, General Counsel, Rural Wireless Association, Inc., to Marlene H. Dortch, Secretary, FCC, WT Docket No. 18-89, at 1-2.

[355] *Id.* at 2.

[356] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[357] United States 5G Leadership Act of 2019, S. 1625, 116th Cong. (2019).

[358] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[359] *See, e.g.*, 47 U.S.C. § 254(e); 47 CFR §§ 54.7, 54.314.

that support only for the provision, maintenance, and upgrading of facilities and services for which the support is intended."[360] We propose that the annual certification should be signed by a duly authorized individual from the company under the penalty of perjury. We believe this proposal will protect the Universal Service Fund and any other potential source of funding from waste, fraud, and abuse. We seek comment on this and other ways to reduce the risk of waste, fraud, and abuse.

149. For instance, to ensure effective use of replacement funding, we propose to adopt a detailed reimbursement application process to confirm that funding is being used only to replace covered equipment and services, rather than to deploy services to new areas or replace aging equipment or services that are not covered. This is similar to the process adopted in the recent spectrum incentive auction where the Commission required broadcasters to submit estimated construction plans to the Media Bureau for the reimbursement of relocation costs.[361] Under the Commission's proposal, applications for replacement funding would need to provide details of the covered equipment and services being replaced, the replacement equipment and services, and the estimated costs of replacement. We seek comment on this proposal.

150. We believe that a detailed application process will verify the original costs, as well as the new replacement costs to ensure USF support or other funding is not wasted and used appropriately for comparable replacement facilities and services or limited upgrades, if the Commission so allows. How do we verify the original and replacement costs to ensure that USF support or other funding is not wasted? What other information should the Commission require and how do we ensure the application process is simple enough that it does not discourage participation or delay efforts to replace equipment and services from covered companies that pose a national security risk? Alternatively, we seek comment on whether we should require affected entities to submit detailed requests for funding as well as detailed invoices similar to the process used within the E-Rate program. Would this option be more efficient than the detailed application process we propose? How do we limit the burden on small entities while safeguarding the available funding? To prevent waste, fraud, and abuse, and to ensure transparency in the reimbursement program, should the Commission make disbursements to eligible entities public as was done following the broadcast incentive auction?[362]

151. As with the existing USF programs, we propose that recipients of support be subject to periodic compliance audits and other inquiries, including as appropriate investigations, to ensure compliance with the Commission's rules and orders.[363] We seek comment on this proposal and whether such an approach is sufficient to encourage compliance.

152. If a recipient violates the proposed condition upon receiving support or includes inappropriate costs in seeking replacement assistance, what steps should we take in response? Are there any mitigating factors that should be considered when taking such steps? Should we impose additional penalties beyond loss of funding and potential forfeitures under section 503 of the Act?[364] For instance, should violators be suspended or barred from receiving USF support? We seek comment on how to align such a penalty with Congress' direction in the 2019 NDAA to ensure that communications services to users and customers is sustained.

153. *Timelines for Removing and Replacing Equipment*. We seek comment on the timing and deadlines for replacement of covered equipment and services by ETCs. We specifically seek comment on

[360] 47 U.S.C. § 254(e).

[361] *See, e.g.*, 47 CFR § 73.3700 (Post-Incentive Auction Licensing and Operation).

[362] *See* FCC, Incentive Auction Dashboard, https://auctiondata.fcc.gov/public/projects/1000 (last visited Nov. 18, 2019).

[363] *See, e.g.*, 47 CFR § 54.320(a).

[364] 47 U.S.C. §§ 254, 503.

the amount of time that may be necessary to replace covered equipment and services currently in communications networks with permissible, equivalent authorized equipment and services. We also seek comment on whether there are other sources of information that we should consider to help inform our decisions on replacement timing and deadlines and to understand the scope of the effort.

154. Should we allow ETCs to obtain support even if they currently use covered equipment and services so long as they agree to replace such equipment and services by a set deadline? This would allow recipients to continue to receive support going forward and thus allow for a transition period to come into compliance without causing a disruption in annual funding for much needed supported services. If so, we propose to set a deadline by which covered equipment and services must be removed as a condition of receiving support. We seek comment on this proposal. How much time should the Commission allow for equipment and service replacement? Does a two-year period provide sufficient time? Or would a longer transition period, such as 3 to 7 years as suggested by one commenter, be more appropriate?[365] We also request comment on how a deadline would impact overall replacement costs.

155. In adopting a deadline, should we require all equipment and services to be removed by a set date, or implement a phased approach with different deadlines for affected ETCs to replace equipment and services? Recognizing the important national security interest in removing covered equipment and services as quickly as possible, if the Commission adopts a phased approach, how long would affected companies need to comply? Should different categories of ETCs be given additional time to replace covered equipment and services? For example, how should the size of the ETC affect the deadline?

156. If we do adopt a phased deadline approach, we seek comment on how to structure the deadlines. Should the Commission identify specific replacement thresholds, or prioritize replacement of certain equipment and services first? How would a transition with set thresholds to replace equipment and services impact ETCs as compared to a single deadline? For any proposed timeline, we seek comment on the impact of the timeline on reimbursement costs. How does the replacement cost of covered equipment and services change over different transition timeframes? Is it more cost-efficient to set a specific deadline or wait for the end of life of the deployed equipment? For example, the record shows support for having a transition period.[366] Alternatively, what are the potential impacts on carriers and consumers of requiring an expedited transition period? Commenters, particularly small wireless carriers, argue that equipment may not be readily available or may only be available at a much higher cost.[367] How do we best model the cost differences based on the timing? How should we factor in potential executive or legislative actions that could have timing and cost implications in the future, such as the additions of further prohibited equipment manufacturers in future legislation?

157. To the extent we allow ETCs to replace covered equipment and services pursuant to varying deadlines while still continuing to receive USF support, should ETCs be allowed to replace a certain percentage of the prohibited equipment and services in the first year in order to continue to receive support for replacement? What types of reporting from these entities would be necessary for the Commission to track compliance with any milestones? If there are reasons outside of an entity's control that delay replacement, should we establish a mechanism for the entity to report noncompliance with the milestones without penalty? Should we provide financial incentives for entities that can accelerate replacement faster than our milestones?

158. *Additional Issues Arising from the 2019 NDAA*. Section 889(b)(2) of the NDAA requires the Commission to prioritize "technical support" to assist affected entities in transitioning from using

[365] Letter from Sarah Tyree, Vice President, Policy and Public Affairs, CoBank, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 18-89, Exh. 1, at 2 (filed July 1, 2019).

[366] *See* CCA Comments at 5; NTCA Public Notice Comments at 10; RWA Public Notice Reply Comments at 16-17.

[367] *See, e.g.*, ITTA Comments at 4-5 (noting that the rule itself could result in price crunches by limiting availability).

covered equipment to new equipment without impacting communications service to consumers.[368] We seek comment on what "technical support" means. Is the Commission or USAC properly suited to provide technical support to carriers as they eliminate covered equipment or services from their network? If so, what "technical support" should the Commission provide to assist affected entities in their transition? We seek comment on how to comply with this portion of section 889(b)(2) of the NDAA. For instance, we seek comment on best practices to reduce the risk from existing equipment and services provided by covered entities while USF recipients transition to safer and more secure equipment and services. Are there ways USF recipients can upgrade software from a covered company to reasonably improve the security of and reduce threats from covered equipment or services? Should recipients be permitted to replace a covered company's software with that of a trusted third party, in a way that could mitigate the security risk? How would such actions reduce the risk and are there ways for the Commission to provide assistance in making these decisions?

159. We also seek comment on how to implement the direction under the 2019 NDAA in light of actions taken by the Executive Branch since August 2018. In particular, on May 15, 2019, the President issued Executive Order 13873 prohibiting the acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service by a person subject to United States jurisdiction, where the Department of Commerce has determined that the transaction is subject to the jurisdiction or direction of a foreign adversary and it poses certain risks to the national security of the United States.[369] The next day, the Bureau of Industry and Security of the Department of Commerce added Huawei Technologies, Co. Ltd. to the Export Administration Regulations (EAR) Entity List.[370] It later amended the EAR to create a 90-day temporary general license allowing some continued exports, reexports, and transfers through August 19, 2019,[371] amended the EAR to extend a second time the temporary general license through November 18, 2019,[372] and then subsequently extended the temporary general license a third time through February 16, 2020.[373] The Secretary of Commerce will also be issuing regulations pursuant to this Executive Order.[374]

160. We seek comment on how to ensure that our actions are consistent and in harmony with actions by other government agencies. How do these Executive Branch actions affect this rulemaking? Are there restrictions imposed by the inclusion of companies on the Entity List that accelerate the need for the Commission to act?

B. Cost Benefit Analysis

161. Based on presently available information, we estimate the cost of requiring the removal

[368] *2019 NDAA*, Sec. 889(b)(2), 132 Stat. at 1917.

[369] Executive Order No. 13,873, 84 Fed. Reg. 22689, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019).

[370] Department of Commerce, Bureau of Industry and Security, Addition of Entities to the Entity List, 84 Fed. Reg. 22961 (May 16, 2019). The EAR Entity List is where persons, including entities, designated by the Bureau of Industry and Security, are identified when "there is reasonable cause to believe, based on specific and articulable facts, that the person has been involved, is involved, or poses a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the United States." *Id*.

[371] Department of Commerce, Bureau of Industry and Security, Temporary General License, 84 Fed. Reg. 23468 (May 22, 2019).

[372] Department of Commerce, Bureau of Industry and Security, Temporary General License, 84 Fed. Reg. 43487 (Aug. 21, 2019).

[373] Department of Commerce, Bureau of Industry and Security, Temporary General License, 84 Fed. Reg. 64018 (Nov. 20, 2019).

[374] Executive Order No. 13,873, 84 Fed. Reg. 22689, *Securing the Information and Communications Technology and Services Supply* Chain (May 15, 2019).

and replacement of covered equipment and services within the next two years to be between $600 million and $2.0billion, i.e., adding approximately $440 million to $1.0 billion more to the costs of our action in the Report and Order.[375] In making this estimate, we adopt the assumptions of the cost benefit analysis of the Report and Order, except we assume all carriers accepting universal service support must remove and replace 100%, rather than only 50% to 75%, of their equipment. We assume that the Report and Order will impact investment decisions starting in 2020, so we would see replacements identical to what would occur under attrition at the end of both 2020 and 2021, covering 2 years or 20% of the original equipment, with replacement cost of the remaining 80% of the Huawei or ZTE asset base occurring at the end of the period. Thus, our cost estimate of between $600 million and $2.0 billion is the sum of the present value of three differences: (1) the difference between the two-year cost streams under attrition and under the base case, plus (2) the difference between the cost stream that removal and replacement generates over the next 8 years and the base case cost stream over those 8 years, plus (3) the difference between the cost flows with the replaced capital and the steady-state annuity under the base case from January 1, 2030, out to 2040. If we extend the transition to seven years (instead of two), the costs will decline by $250 million to $590 million. While we acknowledge that the benefits of our proposed actions are difficult to quantify, we expect that they would outweigh the costs. We seek comment on this analysis and any other quantitative or qualitative information available on the costs and benefits of our proposals.

V. INFORMATION COLLECTION ORDER

162. In the Further Notice, we seek 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 our future efforts to protect the communications supply chain, we direct 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.[376] This information collection will aid our review of the record and guide our next steps in this proceeding.

163. We 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.[377]

164. Specifically, we seek information on all equipment and services from Huawei and ZTE that are used or owned by ETCs. ETCs are the subject of our proposed rule (and among USF recipients the most likely to currently own and use equipment and services from Huawei and ZTE). We therefore limit our information collection only to ETCs and will not require cost information from other USF recipients at this time. We 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 we will allow other USF recipients who are not ETCs to participate on a voluntary basis as well.

165. In implementing this 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 this information collection. All submissions must be certified to

[375] This compares to Cobank's removal-and-replacement cost estimate of $1 billion (Cobank Estimate). That estimate applies to rural carriers only and excludes ongoing operational costs, both of which our estimate includes.

[376] Because section 889(f) of the 2019 NDAA identifies specific companies that are prohibited from federal procurements, and the Further Notice below seeks comment on how to implement those and other prohibitions, we specifically seek comment on the extent to which equipment or services from companies identified in Section 889 of the NDAA exist in current networks. *See* Pub. L. 115-232, 132 Stat. 1636, 1918, Secs. 889(f)(2)-(3).

[377] This information collection applies to all subsidiaries and affiliates of ETCs.

ensure the accuracy of the responses.

166. This information collection shall be mandatory for all ETCs and voluntary for others. We direct 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). We expect, 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 this information collection, we direct WCB and OEA to seek any information necessary to verify responses provided by ETCs to this information collection, including by requiring further information from respondents. We direct WCB and OEA to proceed expeditiously with the information collection, including by seeking emergency PRA approval from OMB, if necessary and appropriate.[378]

VI. PROCEDURAL MATTERS

167. *Effective Date*. The rules adopted herein and the initial designations of Huawei Technologies Company and ZTE Corporation as covered companies shall be effective immediately upon publication in the Federal Register. Comments may be filed according to the comment filing procedures described below and shall be filed in PS Docket No. 19-351 for the Huawei final designation proceeding or in PS Docket No. 19-352 for the ZTE final designation proceeding. The requirements for certifications from USF recipients that they are in compliance with the Commission's rule shall be effective on the date announced by public notice following OMB approval.

168. While a rule ordinarily will take effect 30 days after publication in the Federal Register, we find here that good cause exists to expedite the implementation of these rules and to make them effective upon publication in the Federal Register.[379] In finding that good cause exists, we apply 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."[380]

169. We first examine the necessity for immediate implementation. The record before us 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.[381] In addition, expediting our 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.[382]

---

[378] We believe there is good cause for requesting emergency PRA approval from OMB for the reasons described in para 169. Given the nature of the national security concerns, we find that the serious and immediate risks to communications networks likely justify the expedited approval of this information collection.

[379] *See* 5 U.S.C. § 553(d)(3); 47 CFR § 1.427.

[380] *Omnipoint Corp. v. FCC*, 78 F.3d 620, 630 (D.C. Cir. 1996) (quoting *United States v. Gavrilovic*, 551 F.2d 1099, 1105 (8th Cir. 1977)).

[381] *See Amendment of Part 2 of the Commission's Rules,* Memorandum Opinion and Order, 16 FCC Rcd 2799, 2801, para. 6 (2001) (permitting federal use of spectrum band immediately, due to "near term national security requirements noted by NTIA"). *See also Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems,* Memorandum Opinion and Order, 12 FCC Rcd 22665, 22738, para. 156 (1997) (revising rules implementing wireless 911 obligations effective immediately upon Federal Register publication in light of section 1 policy of "promoting the safety of life and property" and in order to "exten[d] the benefits of 911 services to as many wireless phone users as possible").

[382] *Cf. Procedures for Arbitrations Conducted Pursuant to Section 252(e)(5),* Order, 16 FCC Rcd 6231, 6232, para. 6 (2001) (making new rules available immediately where in contemporaneous order Commission had preempted state jurisdiction "and therefore may soon need to begin the process of" applying the new rules).

Against this critical national security concern we balance the concerns of fairness to affected parties—including whether dispensing with this 30-day waiting period will deprive affected parties of "a reasonable time to adjust their behavior before the final rule takes effect."[383] Here, we note that the principal effect of the rules adopted in this 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 this 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 we adopt today do not include any requirements with which USF recipients must immediately comply.

170. While the Commission has today adopted initial designations of Huawei Technologies Company and ZTE Corporation 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, we will provide copies of this Report and Order to both parties or their U.S. agents or affiliates immediately after release.[384]

171. Even were the rules we adopt today to have an immediate impact on USF recipients, we do not believe it would affect our finding here. Many service providers have already made the business decision to purchase equipment from alternative vendors in order to avoid security risks.[385] Given this, and the industry's long-standing knowledge of the risks posed by the installation and purchase of such equipment, we believe that the impact of an immediate effective date would be minimal.[386]

172. 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 we adopt today, we find 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.[387]

173. *Final Regulatory Flexibility Analysis.* As required by the Regulatory Flexibility Act of 1980,[388] the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) of the possible significant economic impact on small entities of the policies and rules, as proposed, addressed in this *Report and Order*. The FRFA is set forth in Appendix C. The Commission will send a copy of this *Report and Order*, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

---

[383] *Omnipoint*, 78 F.3d at 630.

[384] The Commission has recognized that a finding of good cause under section 553(d)(3) can be further supported where "we are serving those entities by overnight mail." *Access Charge Reform Price Cap Performance Review*, 15 FCC Rcd 12962 (2000), *on review of other issues*, *TOPUC v. FCC*, 265 F.3d 313 (5th Cir. 2001). *See also, e.g.*, *Access Charge Reform*, 12 FCC Rcd 22430 (1997); *Federal State Joint Board on Universal Service*, 14 FCC Rcd 377, 384, para. 16 (1998) (changing funding year for USF RHC support mechanism where those affected "will have actual notice of their obligations when the Commission adopts this order").

[385] *See supra* para. 75.

[386] *See also British Am. Commodity Options Corp. v. Bagley*, 552 F.2d 482, 489 (2d Cir. 1977) (good cause exists where the public has been without the protection of a comprehensive regulatory plan in an area fraught with abuses, and those affected have had ample time to prepare themselves for the rule changes).

[387] *See Omnipoint Corp*, 78 F.3d at 630; 5 U.S.C. § 553(d)(3).

[388] *See* 5 U.S.C. § 604.

174. *Paperwork Reduction Act.* 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 are invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

175. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs that these rules are major under the Congressional Review Act, 5 U.S.C. § 804(2). 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).

176. *Regulatory Flexibility Analysis.* As required by the RFA, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules considered in the Notice. This analysis is found in Appendix D. The *Further Notice* seeks comment on a potential new or revised information collection requirement. Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comment on the Notice of Proposed Rulemaking. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Further Notice of Proposed Rulemaking*, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[389]

177. *Ex Parte Presentations*. The proceeding this Further Notice initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[390] 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.

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

---

[389] *See* 5 U.S.C. § 603(a).

[390] 47 CFR §§ 1.1200 *et seq.*

- 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.

179. *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).

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

181. *Contact Person.* For further information, please contact John Visclosky, Competition Policy Division, Wireline Competition Bureau, at John.Visclosky@fcc.gov or (202) 418-0825.

VII. ORDERING CLAUSES

182. 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 this *Report and Order* IS ADOPTED.

183. IT IS FURTHER ORDERED that Part 54 of the Commission's rules IS AMENDED as set forth in Appendix A.

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

185. IT IS FURTHER ORDERED that, pursuant to sections 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 this *Report and Order* in the *Federal Register*.

186. IT IS FURTHER ORDERED that the Commission SHALL SEND a copy of this *Report and Order* to Congress and to the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

187. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Report and Order*, including the Final Regulatory Flexibility Analysis (FRFA), to the Chief Counsel for Advocacy of the Small Business Administration.

188. 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 this Order SHALL BE EFFECTIVE immediately upon OMB approval.

189. IT IS FURTHER ORDERED that, pursuant to the authority contained in sections 1-4, 201(b), and 254 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201(b), 254, this *Further Notice of Proposed Rulemaking* IS ADOPTED.

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

For the reasons set forth above, Part 54 of Title 47 of the Code of Federal Regulations is amended 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.

SUBPART A – GENERAL INFORMATION

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

§ 54.9 Prohibition on use of funds

(a) 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.

APPENDIX B

Draft Proposed Rules for Public Comment

For the reasons set forth above, Part 54 of Title 47 of the Code of Federal Regulations is amended as follows:

PART 54 – UNIVERSAL SERVICE

1. The authority citation for part 54 continues 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.

SUBPART A – GENERAL INFORMATION

2. Amend section 54.9 by adding paragraphs (c) and (d) to read as follows:

§ 54.9 Prohibition on use of funds

* * * * *

(c) Upon adoption of a funded reimbursement mechanism for replacing such equipment or services, Eligible Telecommunications Carriers must certify prior to receiving a funding commitment or support that it does not use covered equipment or services.

(d) For purposes of paragraph (c), covered equipment or services are equipment or services produced or provided by any company designated by the Commission as posing a national security threat to the integrity of communications networks or the communications supply chain.

APPENDIX C

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the Notice of Proposed Rulemaking (*Protecting Against National Security Threats NPRM* or *Notice*) for this proceeding.[2] The Commission sought written public comment on the proposed rule in the *Notice*, including comment on the IRFA. The Commission received only a single comment on the IRFA.[3] Because the Commission amends its rules in this Report and Order (Order), the Commission has included this Final Regulatory Flexibility Analysis (FRFA). This present FRFA conforms to the RFA.[4]

A. Need for, and Objectives of, the Rules

2. Consistent with our obligation to be responsible stewards of the public funds used in the Universal Service Fund (USF) programs and increasing concern about ensuring communications supply chain integrity, the 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.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

3. The Commission received only a single comment addressing the rules and policies proposed in the IRFA in the *Protecting Against National Security Threats NPRM*. In its comments, NTCA asserts that the IRFA "fails to comply" with the basic requirements of the RFA.[5] NTCA further asserts that the IRFA is inadequate, and "offers no description of the compliance requirements, no projection of the cost of credit, no description of alternatives being considered."[6]

4. We disagree. Contrary to NTCA's claims, the IRFA in the *Protecting Against National Security Threats NPRM* included every category required under the RFA.[7] While NTCA asserts that the IRFA includes no description of potential costs or compliance requirements associated with the proposed rules, the IRFA notes that the *Notice* seeks comment on the costs and benefits of the proposed rule, as well as how broadly it should be applied, who should be held liable for the recovery of disbursed funds, and whether and how applicants for USF support may seek a waiver to purchase or continue to use equipment or services provided by a covered entity.[8] Similarly, while NTCA claims that the IRFA includes no description of any alternatives being considered, the IRFA does, in fact, mention the fact that the *Notice* sought comment on alternative approaches to the proposed rule "and any other steps we should consider taking."[9] The IRFA also cites to the portion of the NPRM that "asks whether there are modifications to our proposed rules that would achieve similar national security objectives, while

---

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. §§ 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 847 (1996).

[2] *See Notice,* 33 FCC Rcd at 4058, para. 2.

[3] *See* NTCA Comments at 18-19.

[4] *See* 5 U.S.C. § 604.

[5] NTCA Comments at 18.

[6] NTCA Comments at 19.

[7] *See* 5 U.S.C. § 604.

[8] *See Notice*, 33 FCC Rcd at 4096, Appx. B, para. 56.

[9] *See Notice*, 33 FCC Rcd at 4096, Appx. B, para. 56.

reducing burdens on small entities. For example, the NPRM asks whether there should be a later effective date for the rule as applied to smaller recipients of USF support. We seek comment on any potential modifications and alternatives that would ease the burden of our proposed rules on small entities."[10] The IRFA also reiterates the Commission's intent to "take into account the economic impact on small entities, as identified in comments . . . in reaching our final conclusions and promulgating rules in this proceeding."[11] Contrary to NTCA's claims, the IRFA does indeed include consideration of alternatives to the proposed rules, as well as the potential benefits and costs of these rules with regards to small entities.

C. Response to Comments by the Chief Counsel for Advocacy of the SBA

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[12]

6. The Chief Counsel did not file any comments in response to this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

7. 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.[13] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[14] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[15] 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.[16]

8. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[17] 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.[18] These types of small businesses represent 99.9% of all businesses in the United States which translates to 28.8 million businesses.[19]

---

[10] *Notice*, 33 FCC Rcd at 4096, Appx. B, para. 61.

[11] *Notice*, 33 FCC Rcd at 4096, Appx. B, para. 62.

[12] 5 U.S.C. § 604 (a)(3).

[13] *See* 5 U.S.C. § 604(a)(4).

[14] *See* 5 U.S.C. § 601(6).

[15] *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."

[16] *See* 15 U.S.C. § 632.

[17] *See* 5 U.S.C. § 601(3)-(6).

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

9. 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."[20] 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).[21]

10. 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."[22] U.S. Census Bureau data from the 2012 Census of Governments[23] indicates that there were 90,056 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[24] Of this number there were 37, 132 general purpose governments (county[25], municipal and town or township[26]) with populations of less than 50,000 and 12,184 special purpose governments (independent school districts[27] and special districts[28]) 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.[29] Based on this data we estimate that at least 49,316 local government jurisdictions fall in the category of "small governmental jurisdictions."[30]

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

1. Schools and Libraries

12. As noted, "small entity" includes non-profit and small government entities. Under the schools and libraries universal service support mechanism, which provides support for elementary and secondary schools and libraries, an elementary school is generally "a non-profit institutional day or

(Continued from previous page)

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

[20] 5 U.S.C. § 601(4).

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

[22] 5 U.S.C. § 601(5).

[23] *See* 13 U.S.C. § 161. The Census of Government is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Program Description, Census of Governments, https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=program&id=program.en.COG# .

[24] *See* U.S. Census Bureau, 2012 Census of Governments, Local Governments by Type and State: 2012 - United States-States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG02.US01. Local governmental jurisdictions are classified in two categories - General purpose governments (county, municipal and town or township) and Special purpose governments (special districts and independent school districts).

residential school, that provides elementary education, as determined under state law."[31] A secondary school is generally defined as "a non-profit institutional day or residential school, that provides secondary education, as determined under state law," and not offering education beyond grade 12.[32] A library includes "(1) a public library, (2) a public elementary school or secondary school library, (3) an academic library, (4) a research library . . . , and (5) a private library, but only if the state in which such private library is located determines that the library should be considered a library for the purposes of this definition."[33] For-profit schools and libraries, and schools and libraries with endowments in excess of $50,000,000, are not eligible to receive discounts under the program, nor are libraries whose budgets are not completely separate from any schools.[34] Certain other statutory definitions apply as well.[35] The SBA has defined for-profit, elementary and secondary schools and libraries having $6 million or less in annual receipts as small entities.[36] In funding year 2007, approximately 105,500 schools and 10,950 libraries received funding under the schools and libraries universal service mechanism. Although we are unable to estimate with precision the number of these entities that would qualify as small entities under SBA's size standard, we estimate that fewer than 105,500 schools and 10,950 libraries might be affected annually by our action, under current operation of the program.

2. Healthcare Providers

13. *Offices of Physicians (except Mental Health Specialists)*. This U.S. industry comprises establishments of health practitioners having the degree of M.D. (Doctor of Medicine) or D.O. (Doctor of Osteopathy) primarily engaged in the independent practice of general or specialized medicine (except psychiatry or psychoanalysis) or surgery. These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[37] The SBA has created a size standard for this industry, which is annual receipts of $11 million or less.[38] According to 2012 U.S. Economic Census, 152,468 firms operated throughout the entire year in this industry.[39] Of that number, 147,718 had annual receipts of less than $10 million, while 3,108 firms had annual receipts between $10 million and $24,999,999.[40] Based on this data, we conclude that a

(Continued from previous page)

[25] *See* U.S. Census Bureau, 2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01. There were 2,114 county governments with populations less than 50,000.

[26] *See* U.S. Census Bureau, 2012 Census of Governments, Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States – States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01. There were 18,811 municipal and 16,207 town and township governments with populations less than 50,000.

[27] *See* U.S. Census Bureau, 2012 Census of Governments, Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United States-States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01. There were 12,184 independent school districts with enrollment populations less than 50,000.

[28] *See* U.S. Census Bureau, 2012 Census of Governments, Special District Governments by Function and State: 2012 - United States-States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG09.US01. The U.S. Census Bureau data did not provide a population breakout for special district governments.

[29] *See* U.S. Census Bureau, 2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01; Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States–States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01; Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United States-States, https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01. While U.S. Census Bureau data did not provide a population breakout for special district governments, if the population of less than 50,000 for this category of local government is consistent with the other types of local governments the majority of the 38, 266 special district governments have populations of less than 50,000.

majority of firms operating in this industry are small under the applicable size standard.

14. *Offices of Physicians, Mental Health Specialists*. This U.S. industry comprises establishments of health practitioners having the degree of M.D. (Doctor of Medicine) or D.O. (Doctor of Osteopathy) primarily engaged in the independent practice of psychiatry or psychoanalysis. These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[41] The SBA has established a size standard for businesses in this industry, which is annual receipts of $11 million dollars or less.[42] The U.S. Economic Census indicates that 8,809 firms operated throughout the entire year in this industry.[43] Of that number 8,791 had annual receipts of less than $10 million, while 13 firms had annual receipts between $10 million and $24,999,999.[44] Based on this data, we conclude that a majority of firms in this industry are small under the applicable standard.

15. *Offices of Dentists*. This U.S. industry comprises establishments of health practitioners having the degree of D.M.D. (Doctor of Dental Medicine), D.D.S. (Doctor of Dental Surgery), or D.D.Sc. (Doctor of Dental Science) primarily engaged in the independent practice of general or specialized dentistry or dental surgery. These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers. They can provide either comprehensive preventive, cosmetic, or emergency care, or specialize in a single field of dentistry.[45] The SBA has established a size standard for that industry of annual receipts of $7.5 million or less.[46] The 2012 U.S. Economic Census indicates that 115,268 firms operated in the dental industry throughout the entire year.[47] Of that number 114,417 had annual receipts of less than $5 million, while 651 firms had annual receipts between $5 million and $9,999,999.[48] Based on this data, we conclude that a majority of businesses in the dental industry are small under the applicable standard.

(Continued from previous page)

[30] *Id.*

[31] 47 CFR § 54.500.

[32] *Id*.

[33] *Id*.

[34] 47 CFR § 54.501(a), (b).

[35] *Id.*

[36] 13 CFR § 121.201; NAICS codes 611110 and 519120 (NAICS code 519120 was previously 514120).

[37] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621111 "Offices of Physicians (except Mental Health Specialists)," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621111&search=2012+NAICS+Search&search=2012.

[38] 13 CFR § 121.201, NAICS Code 621111.

[39] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1262SSSZ4, *Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States:* 2012, NAICS code 621111, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621111.

[40] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $11 million or less.

[41] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621112 "Offices of Physicians, Mental Health Specialists," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621112&search=2012+NAICS+Search&search=2012.

[42] 13 CFR § 121.201, NAICS Code 621112.

[43] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621112, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621112.

16. *Offices of Chiropractors*. This U.S. industry comprises establishments of health practitioners having the degree of D.C. (Doctor of Chiropractic) primarily engaged in the independent practice of chiropractic. These practitioners provide diagnostic and therapeutic treatment of neuromusculoskeletal and related disorders through the manipulation and adjustment of the spinal column and extremities, and operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[49] The SBA has established a size standard for this industry, which is annual receipts of $7.5 million or less.[50] The 2012 U.S. Economic Census statistics show that 33,940 firms operated throughout the entire year.[51] Of that number 33,910 operated with annual receipts of less than $5 million per year, while 26 firms had annual receipts between $5 million and $9,999,999.[52] Based on that data, we conclude that a majority of chiropractors are small.

17. *Offices of Optometrists*. This U.S. industry comprises establishments of health practitioners having the degree of O.D. (Doctor of Optometry) primarily engaged in the independent practice of optometry. These practitioners examine, diagnose, treat, and manage diseases and disorders of the visual system, the eye and associated structures as well as diagnose related systemic conditions. Offices of optometrists prescribe and/or provide eyeglasses, contact lenses, low vision aids, and vision therapy. They operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers, and may also provide the same services as opticians, such as selling and fitting prescription eyeglasses and contact lenses.[53] The SBA has established a size standard for businesses operating in this industry, which is annual receipts of $7.5 million or less.[54] The 2012 Economic Census indicates that 18,050 firms operated the entire year.[55] Of that number, 17,951 had annual receipts of less than $5 million, while 70 firms had annual receipts

(Continued from previous page)

[44] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $11 million or less.

[45] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621210 "Offices of Dentists," https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621210&search=2012+NAICS+Search&search=2012.

[46] 13 CFR § 121.201, NAICS Code 621210.

[47] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1262SSSZ4, *Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States:* 2012, NAICS code 621210, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621210.

[48] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[49] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621310 "Offices of Chiropractors", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621310&search=2012+NAICS+Search&search=2012; *see also* 13 CFR § 121.201; NAICS code 621310.

[50] 13 CFR § 121.201, NAICS Code 621310.

[51] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1262SSSZ4, *Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621310, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621310.

[52] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

between $5 million and $9,999,999.[56] Based on this data, we conclude that a majority of optometrists in this industry are small.

18. *Offices of Mental Health Practitioners (except Physicians)*. This U.S. industry comprises establishments of independent mental health practitioners (except physicians) primarily engaged in (1) the diagnosis and treatment of mental, emotional, and behavioral disorders and/or (2) the diagnosis and treatment of individual or group social dysfunction brought about by such causes as mental illness, alcohol and substance abuse, physical and emotional trauma, or stress. These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[57] The SBA has created a size standard for this industry, which is annual receipts of $7.5 million or less.[58] The 2012 U.S. Economic Census indicates that 16,058 firms operated throughout the entire year.[59] Of that number, 15,894 firms received annual receipts of less than $5 million, while 111 firms had annual receipts between $5 million and $9,999,999.[60] Based on this data, we conclude that a majority of mental health practitioners who do not employ physicians are small.

19. *Offices of Physical, Occupational and Speech Therapists and Audiologists*. This U.S. industry comprises establishments of independent health practitioners primarily engaged in one of the following: (1) providing physical therapy services to patients who have impairments, functional limitations, disabilities, or changes in physical functions and health status resulting from injury, disease or other causes, or who require prevention, wellness or fitness services; (2) planning and administering educational, recreational, and social activities designed to help patients or individuals with disabilities, regain physical or mental functioning or to adapt to their disabilities; and (3) diagnosing and treating speech, language, or hearing problems. These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[61] The SBA has established a size standard for this industry, which is annual receipts of $7.5 million or less.[62] The 2012 U.S. Economic Census indicates that 20,567 firms in this industry operated throughout the entire year.[63] Of that number, 20,047 had annual receipts of less than $5 million, while 270 firms had

(Continued from previous page)

[53] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621320 "Offices of Optometrists", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621320&search=2012+NAICS+Search&search=2012.

[54] 13 CFR § 121.201, NAICS code 621320.

[55] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621320, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621320.

[56] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[57] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621330 "Offices of Mental Health Practitioners (except Physicians)", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621330&search=2012+NAICS+Search&search=2012.

[58] 13 CFR § 121.201, NAICS Code 621330.

[59] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621330, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621330.

[60] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[61] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621340 "Offices of Physical, Occupational and Speech Therapists and Audiologists", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621340&search=2012+NAICS+Search&search=2012.

[62] 13 CFR § 121.201, NAICS Code 621340.

annual receipts between $5 million and $9,999,999.[64] Based on this data, we conclude that a majority of businesses in this industry are small.

20. *Offices of Podiatrists*. This U.S. industry comprises establishments of health practitioners having the degree of D.P.M. (Doctor of Podiatric Medicine) primarily engaged in the independent practice of podiatry. These practitioners diagnose and treat diseases and deformities of the foot and operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[65] The SBA has established a size standard for businesses in this industry, which is annual receipts of $7.5 million or less.[66] The 2012 U.S. Economic Census indicates that 7,569 podiatry firms operated throughout the entire year.[67] Of that number, 7,545 firms had annual receipts of less than $5 million, while 22 firms had annual receipts between $5 million and $9,999,999.[68] Based on this data, we conclude that a majority of firms in this industry are small.

21. *Offices of All Other Miscellaneous Health Practitioners*. This U.S. industry comprises establishments of independent health practitioners (except physicians; dentists; chiropractors; optometrists; mental health specialists; physical, occupational, and speech therapists; audiologists; and podiatrists). These practitioners operate private or group practices in their own offices (e.g., centers, clinics) or in the facilities of others, such as hospitals or HMO medical centers.[69] The SBA has established a size standard for this industry, which is annual receipts of $7.5 million or less.[70] The 2012 U.S. Economic Census indicates that 11,460 firms operated throughout the entire year.[71] Of that number, 11,374 firms had annual receipts of less than $5 million, while 48 firms had annual receipts between $5 million and $9,999,999.[72] Based on this data, we conclude the majority of firms in this industry are small.

22. *Family Planning Centers*. This U.S. industry comprises establishments with medical staff primarily engaged in providing a range of family planning services on an outpatient basis, such as contraceptive services, genetic and prenatal counseling, voluntary sterilization, and therapeutic and medically induced termination of pregnancy.[73] The SBA has established a size standard for this industry,

(Continued from previous page)

[63] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621340, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621340.

[64] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[65] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621391 "Offices of Podiatrists", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621391&search=2012+NAICS+Search&search=2012.

[66] 13 CFR § 121.201, NAICS Code 621391.

[67] U.S. Census Bureau, 2012 Economic Census of the United States, Table EC1262SSSZ4, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States: 2012, NAICS code 621391, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621391.

[68] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[69] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621399 "Offices of All Other Miscellaneous Health Practitioners", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621399&search=2012+NAICS+Search&search=2012.

[70] 13 CFR § 121.201, NAICS Code 621399.

[71] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4, *Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621399, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621399.

which is annual receipts of $11 million or less.[74] The 2012 Economic Census indicates that 1,286 firms in this industry operated throughout the entire year.[75] Of that number 1,237 had annual receipts of less than $10 million, while 36 firms had annual receipts between $10 million and $24,999,999.[76] Based on this data, we conclude that the majority of firms in this industry are small.

23. *Outpatient Mental Health and Substance Abuse Centers*. This U.S. industry comprises establishments with medical staff primarily engaged in providing outpatient services related to the diagnosis and treatment of mental health disorders and alcohol and other substance abuse. These establishments generally treat patients who do not require inpatient treatment. They may provide a counseling staff and information regarding a wide range of mental health and substance abuse issues and/or refer patients to more extensive treatment programs, if necessary.[77] The SBA has established a size standard for this industry, which is $15 million or less in annual receipts.[78] The 2012 U.S. Economic Census indicates that 4,446 firms operated throughout the entire year.[79] Of that number, 4,069 had annual receipts of less than $10 million while 286 firms had annual receipts between $10 million and $24,999,999.[80] Based on this data, we conclude that a majority of firms in this industry are small.

24. *HMO Medical Centers*. This U.S. industry comprises establishments with physicians and other medical staff primarily engaged in providing a range of outpatient medical services to the health maintenance organization (HMO) subscribers with a focus generally on primary health care. These establishments are owned by the HMO. Included in this industry are HMO establishments that both provide health care services and underwrite health and medical insurance policies.[81] The SBA has established a size standard for this industry, which is $32.5 million or less in annual receipts.[82] The 2012 U.S. Economic Census indicates that 14 firms in this industry operated throughout the entire year.[83] Of that number, 5 firms had annual receipts of less than $25 million, while 1 firm had annual receipts

(Continued from previous page)

[72] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $7.5 million or less.

[73] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621410 "Family Planning Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621410&search=2012+NAICS+Search&search=2012.

[74] 13 CFR § 121.201, NAICS Code 621410.

[75] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621410, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621410.

[76] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $11 million or less.

[77] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621420 "Outpatient Mental Health and Substance Abuse Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621420&search=2012+NAICS+Search&search=2012.

[78] 13 CFR § 121.201, NAICS Code 621420.

[79] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621420, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621420.

[80] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

between $25 million and $99,999,999.[84] Based on this data, we conclude that approximately one-third of the firms in this industry are small.

25. *Freestanding Ambulatory Surgical and Emergency Centers*. This U.S. industry comprises establishments with physicians and other medical staff primarily engaged in (1) providing surgical services (e.g., orthoscopic and cataract surgery) on an outpatient basis or (2) providing emergency care services (e.g., setting broken bones, treating lacerations, or tending to patients suffering injuries as a result of accidents, trauma, or medical conditions necessitating immediate medical care) on an outpatient basis. Outpatient surgical establishments have specialized facilities, such as operating and recovery rooms, and specialized equipment, such as anesthetic or X-ray equipment.[85] The SBA has established a size standard for this industry, which is annual receipts of $15 million or less.[86] The 2012 U.S. Economic Census indicates that 3,595 firms in this industry operated throughout the entire year.[87] Of that number, 3,222 firms had annual receipts of less than $10 million, while 289 firms had annual receipts between $10 million and $24,999,999.[88] Based on this data, we conclude that a majority of firms in this industry are small.

26. *All Other Outpatient Care Centers*. This U.S. industry comprises establishments with medical staff primarily engaged in providing general or specialized outpatient care (except family planning centers, outpatient mental health and substance abuse centers, HMO medical centers, kidney dialysis centers, and freestanding ambulatory surgical and emergency centers). Centers or clinics of health practitioners with different degrees from more than one industry practicing within the same establishment (i.e., Doctor of Medicine and Doctor of Dental Medicine) are included in this industry.[89] The SBA has established a size standard for this industry, which is annual receipts of $20.5 million or less.[90] The 2012 U.S. Economic Census indicates that 4,903 firms operated in this industry throughout the entire year.[91] Of this number, 4,269 firms had annual receipts of less than $10 million, while 389

(Continued from previous page)

[81] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621491 "HMO Medical Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621491&search=2012+NAICS+Search&search=2012.

[82] 13 CFR § 121.201, NAICS code 621491.

[83] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621491, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621491.

[84] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $32.5 million or less.

[85] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621493 "Freestanding Ambulatory Surgical and Emergency Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621493&search=2012+NAICS+Search&search=2012.

[86] 13 CFR § 121.201, NAICS Code 621493.

[87] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621493, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621493.

[88] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

[89] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621498 "All Other Outpatient Care Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621498&search=2012+NAICS+Search&search=2012.

[90] 13 CFR § 121.201, NAICS Code 621498.

firms had annual receipts between $10 million and $24,999,999.[92] Based on this data, we conclude that a majority of firms in this industry are small.

27. *Blood and Organ Banks*. This U.S. industry comprises establishments primarily engaged in collecting, storing, and distributing blood and blood products and storing and distributing body organs.[93] The SBA has established a size standard for this industry, which is annual receipts of $32.5 million or less.[94] The 2012 U.S. Economic Census indicates that 314 firms operated in this industry throughout the entire year.[95] Of that number, 235 operated with annual receipts of less than $25 million, while 41 firms had annual receipts between $25 million and $49,999,999.[96] Based on this data, we conclude that approximately three-quarters of firms that operate in this industry are small.

28. *All Other Miscellaneous Ambulatory Health Care Services*. This U.S. industry comprises establishments primarily engaged in providing ambulatory health care services (except offices of physicians, dentists, and other health practitioners; outpatient care centers; medical and diagnostic laboratories; home health care providers; ambulances; and blood and organ banks).[97] The SBA has established a size standard for this industry, which is annual receipts of $15 million or less.[98] The 2012 U.S. Economic Census indicates that 2,429 firms operated in this industry throughout the entire year.[99] Of that number, 2,318 had annual receipts of less than $10 million, while 56 firms had annual receipts between $10 million and $24,999,999.[100] Based on this data, we conclude that a majority of the firms in this industry are small.

29. *Medical Laboratories*. This U.S. industry comprises establishments known as medical laboratories primarily engaged in providing analytic or diagnostic services, including body fluid analysis, generally to the medical profession or to the patient on referral from a health practitioner.[101] The SBA has established a size standard for this industry, which is annual receipts of $32.5 million or less.[102] The 2012 U.S. Economic Census indicates that 2,599 firms operated in this industry throughout the entire year.[103] Of this number, 2,465 had annual receipts of less than $25 million, while 60 firms had annual receipts

(Continued from previous page)

[91] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621498, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621498.

[92] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $20.5 million or less.

[93] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621991 "Blood and Organ Banks", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621991&search=2012+NAICS+Search&search=2012.

[94] 13 CFR § 121.201, NAICS Code 621991.

[95] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621991, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621991.

[96] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $32.5 million or less.

[97] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621999 "All Other Miscellaneous Ambulatory Health Care Services", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621999&search=2012+NAICS+Search&search=2012.

[98] 13 CFR § 121.201, NAICS Code 621999.

[99] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621999, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621999.

[100] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

between $25 million and $49,999,999.[104] Based on this data, we conclude that a majority of firms that operate in this industry are small.

30. *Diagnostic Imaging Centers*. This U.S. industry comprises establishments known as diagnostic imaging centers primarily engaged in producing images of the patient generally on referral from a health practitioner.[105] The SBA has established size standard for this industry, which is annual receipts of $15 million or less.[106] The 2012 U.S. Economic Census indicates that 4,209 firms operated in this industry throughout the entire year.[107] Of that number, 3,876 firms had annual receipts of less than $10 million, while 228 firms had annual receipts between $10 million and $24,999,999.[108] Based on this data, we conclude that a majority of firms that operate in this industry are small.

31. *Home Health Care Services*. This U.S. industry comprises establishments primarily engaged in providing skilled nursing services in the home, along with a range of the following: personal care services; homemaker and companion services; physical therapy; medical social services; medications; medical equipment and supplies; counseling; 24-hour home care; occupation and vocational therapy; dietary and nutritional services; speech therapy; audiology; and high-tech care, such as intravenous therapy.[109] The SBA has established a size standard for this industry, which is annual receipts of $15 million or less.[110] The 2012 U.S. Economic Census indicates that 17,770 firms operated in this industry throughout the entire year.[111] Of that number, 16,822 had annual receipts of less than $10 million, while 590 firms had annual receipts between $10 million and $24,999,999.[112] Based on this data, we conclude that a majority of firms that operate in this industry are small.

32. *Ambulance Services*. This U.S. industry comprises establishments primarily engaged in providing transportation of patients by ground or air, along with medical care. These services are often provided during a medical emergency but are not restricted to emergencies. The vehicles are equipped with lifesaving equipment operated by medically trained personnel.[113] The SBA has established a size standard for this industry, which is annual receipts of $15 million or less.[114] The 2012 U.S. Economic

(Continued from previous page)

[101] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621511 "Medical Laboratories", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621511&search=2012+NAICS+Search&search=2012.

[102] 13 CFR § 121.201, NAICS Code 621511.

[103] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621511, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621511.

[104] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $32.5 million or less.

[105] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621512 "Diagnostic Imaging Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621512&search=2012+NAICS+Search&search=2012.

[106] 13 CFR § 121.201, NAICS Code 621512.

[107] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621512, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621512.

[108] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

[109] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621610 "Home Health Care Services", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621610&search=2012+NAICS+Search&search=2012.

[110] 13 CFR § 121.201, NAICS Code 621610.

Census indicates that 2,984 firms operated in this industry throughout the entire year.[115] Of that number, 2,926 had annual receipts of less than $15 million, while 133 firms had annual receipts between $10 million and $24,999,999.[116] Based on this data, we conclude that a majority of firms in this industry are small.

33. *Kidney Dialysis Centers*. This U.S. industry comprises establishments with medical staff primarily engaged in providing outpatient kidney or renal dialysis services.[117] The SBA has established assize standard for this industry, which is annual receipts of $38.5 million or less.[118] The 2012 U.S. Economic Census indicates that 396 firms operated in this industry throughout the entire year.[119] Of that number, 379 had annual receipts of less than $25 million, while 7 firms had annual receipts between $25 million and $49,999,999.[120] Based on this data, we conclude that a majority of firms in this industry are small.

34. *General Medical and Surgical Hospitals*. This U.S. industry comprises establishments known and licensed as general medical and surgical hospitals primarily engaged in providing diagnostic and medical treatment (both surgical and nonsurgical) to inpatients with any of a wide variety of medical conditions. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. These hospitals have an organized staff of physicians and other medical staff to provide patient care services. These establishments usually provide other services, such as outpatient services, anatomical pathology services, diagnostic X-ray services, clinical laboratory services, operating room services for a variety of procedures, and pharmacy services.[121] The SBA has established a size standard for this industry, which is annual receipts of $38.5 million or less.[122] The 2012 U.S. Economic Census indicates that 2,800 firms operated in this industry throughout the entire year.[123] Of that number, 877 has annual receipts of less than $25 million, while 400 firms had annual receipts

(Continued from previous page)

[111] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621610, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621610.

[112] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

[113] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621910 "Ambulance Services", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621910&search=2012+NAICS+Search&search=2012.

[114] 13 CFR § 121.201, NAICS Code 621910.

[115] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621910, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621910.

[116] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $15 million or less.

[117] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 621492 "Kidney Dialysis Centers", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=621492&search=2012+NAICS+Search&search=2012.

[118] 13 CFR § 121.201, NAICS Code 621492.

[119] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 621492, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~621492.

between $25 million and $49,999,999.[124] Based on this data, we conclude that approximately one-quarter of firms in this industry are small.

35. *Psychiatric and Substance Abuse Hospitals*. This U.S. industry comprises establishments known and licensed as psychiatric and substance abuse hospitals primarily engaged in providing diagnostic, medical treatment, and monitoring services for inpatients who suffer from mental illness or substance abuse disorders. The treatment often requires an extended stay in the hospital. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. They have an organized staff of physicians and other medical staff to provide patient care services. Psychiatric, psychological, and social work services are available at the facility. These hospitals usually provide other services, such as outpatient services, clinical laboratory services, diagnostic X-ray services, and electroencephalograph services.[125] The SBA has established a size standard for this industry, which is annual receipts of $38.5 million or less.[126] The 2012 U.S. Economic Census indicates that 404 firms operated in this industry throughout the entire year.[127] Of that number, 185 had annual receipts of less than $25 million, while 107 firms had annual receipts between $25 million and $49,999,999.[128] Based on this data, we conclude that more than one-half of the firms in this industry are small.

36. *Specialty (Except Psychiatric and Substance Abuse) Hospitals*. This U.S. industry consists of establishments known and licensed as specialty hospitals primarily engaged in providing diagnostic, and medical treatment to inpatients with a specific type of disease or medical condition (except psychiatric or substance abuse). Hospitals providing long-term care for the chronically ill and hospitals providing rehabilitation, restorative, and adjustive services to physically challenged or disabled people are included in this industry. These establishments maintain inpatient beds and provide patients with food services that meet their nutritional requirements. They have an organized staff of physicians and other medical staff to provide patient care services. These hospitals may provide other services, such as outpatient services, diagnostic X-ray services, clinical laboratory services, operating room services, physical therapy services, educational and vocational services, and psychological and social work

(Continued from previous page)

[120] *Id*. The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $38.5 million or less.

[121] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 622110 "General Medical and Surgical Hospitals", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=622110&search=2012+NAICS+Search&search=2012.

[122] 13 CFR § 121.201, NAICS Code 622110.

[123] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 622110, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~622110.

[124] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $38.5 million or less.

[125] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 622210 "Psychiatric and Substance Abuse Hospitals", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=622210&search=2012+NAICS+Search&search=2012.

[126] 13 CFR § 121.201, NAICS Code 622210.

[127] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 622210, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~622210.

[128] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $38.5 million or less.

services.[129] The SBA has established a size standard for this industry, which is annual receipts of $38.5 million or less.[130] The 2012 U.S. Economic Census indicates that 346 firms operated in this industry throughout the entire year.[131] Of that number, 146 firms had annual receipts of less than $25 million, while 79 firms had annual receipts between $25 million and $49,999,999.[132] Based on this data, we conclude that more than one-half of the firms in this industry are small.

37. *Emergency and Other Relief Services*. This industry comprises establishments primarily engaged in providing food, shelter, clothing, medical relief, resettlement, and counseling to victims of domestic or international disasters or conflicts (e.g., wars).[133] The SBA has established a size standard for this industry which is annual receipts of $32.5 million or less.[134] The 2012 U.S. Economic Census indicates that 541 firms operated in this industry throughout the entire year.[135] Of that number, 509 had annual receipts of less than $25 million, while 7 firms had annual receipts between $25 million and $49,999,999.[136] Based on this data, we conclude that a majority of firms in this industry are small.

3. Providers of Telecommunications and Other Services

a. Telecommunications Service Providers

38. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers and under the SBA size standard, such a business is small if it has 1,500 or fewer employees.[137] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year. Of this total, 3,083 operated with fewer than 1,000 employees.[138] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[139] Of this total, an estimated 1,006 have 1,500 or fewer

---

[129] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 622310 "Specialty (Except Psychiatric and Substance Abuse) Hospitals", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=622310&search=2012+NAICS+Search&search=2012.

[130] 13 CFR § 121.201, NAICS Code 622310.

[131] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 622310, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~622310.

[132] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $38.5 million or less.

[133] *See* U.S. Census Bureau, 2012 NAICS Definitions, NAICS Code 624230 "Emergency and Other Relief Services", https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=624230&search=2012+NAICS+Search&search=2012.

[134] 13 CFR § 121.201, NAICS Code 624230.

[135] U.S. Census Bureau, *2012 Economic Census of the United States,* Table EC1262SSSZ4*, Healthcare and Social Assistance: Subject Series - Estab and Firm Size: Receipts/Revenue Size of Firms for the United States*: 2012, NAICS code 624230, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/62SSSZ4//naics~624230.

[136] *Id.* The available U.S. Census data does not provide a more precise estimate of the number of firms that meet the SBA size standard of annual receipts of $32.5 million or less.

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

employees.[140] Thus using the SBA's size standard the majority of Incumbent LECs can be considered small entities.

39. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to providers of interexchange services (IXCs). The closest NAICS Code category is Wired Telecommunications Carriers and the applicable size standard under SBA rules consists of all such companies having 1,500 or fewer employees.[141] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[142] Of that number, 3,083 operated with fewer than 1,000 employees.[143] According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services.[144] Of this total, an estimated 317 have 1,500 or fewer employees.[145] Consequently, the Commission estimates that the majority of interexchange service providers that may be affected are small entities.

40. *Competitive Access Providers*. Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to competitive access services providers (CAPs). The closest applicable definition under the SBA rules is Wired Telecommunications Carriers and under the size standard, such a business is small if it has 1,500 or fewer employees.[146] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[147] Of that number, 3,083 operated with fewer than 1,000 employees.[148] Consequently, the Commission estimates that most competitive access providers are small businesses that may be affected by our actions. According to Commission data the *2010 Trends in Telephone Report*, 1,442 CAPs and competitive local exchange carriers (competitive LECs) reported that they were engaged in the provision of competitive local exchange services.[149] Of these 1,442 CAPs and competitive LECs, an estimated 1,256 have 1,500 or fewer employees and 186 have more than 1,500 employees.[150] Consequently, the Commission estimates that most providers of

(Continued from previous page)

[138] *Id*.

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

[140] *Id*.

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

[142] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[143] *Id*.

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

[145] *Id*.

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

[147] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[148] *Id*.

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

competitive exchange services are small businesses.

41. *Operator Service Providers (OSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate category for Operator Service Providers is the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[151] Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[152] Thus, under this size standard, the majority of firms in this industry can be considered small. According to Commission data, 33 carriers have reported that they are engaged in the provision of operator services.[153] Of these, an estimated 31 have 1,500 or fewer employees and two have more than 1,500 employees.[154] Consequently, the Commission estimates that the majority of OSPs are small entities that may be affected by the adopted rules.

42. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[155] Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees.[156] Census Bureau data from 2012 show that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees.[157] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[158] Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees.[159] Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the adopted rules.

43. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and

(Continued from previous page)

[150] *Id.*

[151] 13 CFR § 121.201. The Wired Telecommunications Carrier category formerly used the NAICS code of 517110. As of 2017 the U.S. Census Bureau definition shows the NAICs code as 517311 for Wired Telecommunications Carriers. *See* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[152] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Information: Subject Series - Estab & Firm Size: Receipts Size of Firms for the U.S.: 2012, http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

[153] *Trends in Telephone Service*, tbl. 5.3.

[154] *Id.*

[155] U.S. Census Bureau, 2017 NAICS Definition, 517911 Telecommunications Resellers, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[156] 13 CFR § 121.201, NAICS code 517911.

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

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

[159] *See id*.

operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[160] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[161] Under that size standard, such a business is small if it has 1,500 or fewer employees.[162] Census Bureau data from 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees.[163] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[164] Of this total, an estimated 857 have 1,500 or fewer employees.[165] Consequently, the Commission estimates that the majority of toll resellers are small entities.

44. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including voice over Internet protocol (VoIP)VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[166] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[167] U.S. Census data for 2012 show that there were 3,117 firms that operated that year.[168] Of this total, 3,083 operated with fewer than 1,000 employees.[169] Thus, under this size standard, the majority of firms in this industry can be considered small.

45. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and

---

[160] U.S. Census Bureau, 2017 NAICS Definition, 517911 Telecommunications Resellers, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[161] 13 CFR § 121.201, NAICS code 517911.

[162] *Id.*

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

[164] *Trends in Telephone Service* at tbl. 5.3.

[165] *Id.*

[166] *See* 13 CFR § 120.201. The Wired Telecommunications Carrier category formerly used the NAICS code of 517110. As of 2017 the U.S. Census Bureau definition shows the NAICS code as 517311 for Wired Telecommunications Carriers. *See*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[167] *Id*.

[168] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[169] *Id.*

wireless video services.[170] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[171] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[172] Of this total, 955 firms had employment of 999 or fewer employees and 12 had employment of 1000 employees or more.[173] Thus, under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

46. The Commission's own data—available in its Universal Licensing System—indicate that, as of October 25, 2016, there are 280 Cellular licensees that will be affected by our actions today.[174] The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services.[175] Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees.[176] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

47. *Common Carrier Paging*. As noted, since 2007 the Census Bureau has placed paging providers within the broad economic census category of Wireless Telecommunications Carriers (except Satellite).[177]

48. In addition, in the *Paging Second Report and Order*, the Commission adopted a size standard for "small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[178] A small business is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years.[179] The SBA has approved this definition.[180] An initial auction of Metropolitan Economic Area ("MEA") licenses was conducted in the year 2000. Of the 2,499 licenses auctioned, 985 were sold.[181]

---

[170] NAICS Code 517210. *See* https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.517210.

[171] 13 CFR § 121.201, NAICS code 517210.

[172] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ5, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012 NAICS Code 517210 (rel. Jan. 8, 2016). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517210.

[173] *Id*. Available census data does not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with "1000 employees or more."

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

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

[176] *See id*.

[177] *See* U.S. Census Bureau, 2007 NAICS Definitions, "517210 Wireless Telecommunications Categories (Except Satellite)", http://www.census.gov/naics/2007/def/ND517210.HTM#N517210 (last visited Oct. 24, 2017).

[178] *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems et al.*, WT Docket No. 96-18 et al., Second Report and Order and Further Notice of Proposed Rulemaking, 12 FCC Rcd 2732, 2811-12, paras. 178-81 (1997) (*Paging Second Report and Order*); *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems et al.*, Memorandum Opinion and Order on Reconsideration and Third Report and Order, 14 FCC Rcd 10030, 10085-88, paras. 98-107 (1999).

[179] *Paging Second Report and Order*, 12 FCC Rcd at 2811, para. 179.

Fifty-seven companies claiming small business status won 440 licenses.[182] A subsequent auction of MEA and Economic Area ("EA") licenses was held in the year 2001. Of the 15,514 licenses auctioned, 5,323 were sold.[183] One hundred thirty-two companies claiming small business status purchased 3,724 licenses. A third auction, consisting of 8,874 licenses in each of 175 EAs and 1,328 licenses in all but three of the 51 MEAs, was held in 2003. Seventy-seven bidders claiming small or very small business status won 2,093 licenses.[184]

49. Currently, there are approximately 74,000 Common Carrier Paging licenses. According to the most recent Trends in Telephone Service, 291 carriers reported that they were engaged in the provision of "paging and messaging" services.[185] Of these, an estimated 289 have 1,500 or fewer employees and two have more than 1,500 employees.[186] We estimate that the majority of common carrier paging providers would qualify as small entities under the SBA definition.

50. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services, and specialized mobile radio telephony carriers. The closest applicable SBA category is Wireless Telecommunications Carriers (except Satellite)[187] and the appropriate size standard for this category under the SBA rules is that such a business is small if it has 1,500 or fewer employees.[188] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[189] Of this total, 955 firms had fewer than 1,000 employees and 12 firms has 1000 employees or more.[190] Thus, under this category and the associated size standard, the Commission estimates that a majority of these entities can be considered small. According to Commission data, 413 carriers reported that they were engaged in wireless telephony.[191] Of these, an estimated 261 have 1,500 or fewer employees and 152 have more than 1,500 employees.[192] Therefore, more than half of these entities can be considered small.

51. *Satellite Telecommunications*. This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and

(Continued from previous page)

[180] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (Dec. 2, 1998).

[181] *See 929 and 931 MHz Paging Auction Closes*, Public Notice, 15 FCC Rcd 4858 (WTB 2000).

[182] *See id.*

[183] *See Lower and Upper Paging Bands Auction Closes*, Public Notice, 16 FCC Rcd 21821 (WTB 2001).

[184] *See Lower and Upper Paging Bands Auction Closes*, Public Notice, 18 FCC Rcd 11154 (WTB 2003). The current number of small or very small business entities that hold wireless licenses may differ significantly from the number of such entities that won in spectrum auctions due to assignments and transfers of licenses in the secondary market over time. In addition, some of the same small business entities may have won licenses in more than one auction.

[185] *2010 Trends Report* at Table 5.3, page 5-5.

[186] *Id*.

[187] 13 CFR § 121.201, NAICS code 517210.

[188] *Id*.

[189] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ5, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012 NAICS Code 517210 (rel. Jan. 8, 2016). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517210.

[190] *Id*. Available census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with "1000 employees or more."

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

[192] *Id*.

broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[193] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $32.5 million or less in average annual receipts, under SBA rules.[194] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[195] Of this total, 299 firms had annual receipts of less than $25 million.[196] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

52. *All Other Telecommunications*. The "All Other Telecommunications" category is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[197] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[198] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[199] The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less.[200] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[201] Of these firms, a total of 1,400 had gross annual receipts of less than $25 million and 42 firms had gross annual receipts of $25 million to $49, 999,999.[202] Thus, the Commission estimates that a majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

b. Internet Service Providers

53. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications infrastructure fall in the category of Wired Telecommunication Carriers.[203] Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data,

---

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

[194] 13 CFR § 121.201, NAICS code 517410.

[195] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517410 https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ4//naics~517410.

[196] *Id*.

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

[198] *Id*.

[199] *Id*.

[200] 13 CFR § 121.201; NAICS Code 517919.

[201] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517919, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ4//naics~517919.

[202] *Id*.

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

text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies.[204] The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees.[205] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[206] Consequently, under this size standard the majority of firms in this industry can be considered small.

54. *Internet Service Providers (Non-Broadband)*. Internet access service providers such as Dial-up Internet service providers, VoIP service providers using client-supplied telecommunications connections and Internet service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) fall in the category of All Other Telecommunications. The SBA has developed a small business size standard for All Other Telecommunications which consists of all such firms with gross annual receipts of $32.5 million or less.[207] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[208] Consequently, under this size standard, a majority of firms in this industry can be considered small.

c. Vendors and Equipment Manufacturers

55. *Vendors of Infrastructure Development or "Network Buildout."* The Commission has not developed a small business size standard specifically directed toward manufacturers of network facilities. There are two applicable SBA categories in which manufacturers of network facilities could fall and each have different size standards under the SBA rules. The SBA categories are "Radio and Television Broadcasting and Wireless Communications Equipment" with a size standard of 1,250 employees or less[209] and "Other Communications Equipment Manufacturing" with a size standard of 750 employees or less."[210] U.S. Census Bureau data for 2012 show that for Radio and Television Broadcasting and Wireless Communications Equipment firms 841 establishments operated for the entire year.[211] Of that number, 828 establishments operated with fewer than 1,000 employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments operated with 2,500 or more employees.[212] For Other Communications Equipment Manufacturing, U.S. Census Bureau data for 2012

---

[204] *Id.*

[205] *Id.*

[206] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size, NAICS code 334290, http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

[207] 13 CFR § 121.201; NAICS Code 517919.

[208] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab & Firm Size: Receipts Size of Firms for the U.S.: 2012, NAICS Code 517919, https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

[209] 13 CFR § 121.201, NAICS Code 334220.

[210] 13 CFR § 121.201, NAICS Code 334290.

[211] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334220, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334220.

[212] *Id*.

show that 383 establishments operated for the year.[213] Of that number 379 firms operated with fewer than 500 employees and 4 had 500 to 999 employees. Based on this data, we conclude that the majority of Vendors of Infrastructure Development or "Network Buildout" are small.

56. *Telephone Apparatus Manufacturing*. This industry comprises establishments primarily engaged in manufacturing wire telephone and data communications equipment. These products may be standalone or board-level components of a larger system. Examples of products made by these establishments are central office switching equipment, cordless telephones (except cellular), PBX equipment, telephones, telephone answering machines, LAN modems, multi-user modems, and other data communications equipment, such as bridges, routers, and gateways."[214] The SBA size standard for Telephone Apparatus Manufacturing is all such firms having 1,250 or fewer employees.[215] According to U.S. Census Bureau data for 2012, there were a total of 266 establishments in this category that operated for the entire year.[216] Of this total, 262 had employment of under 1,000, and an additional 4 had employment of 1,000 to 2,499.[217] Thus, under this size standard, the majority of firms can be considered small.

57. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[218] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[219] The SBA has established a small business size standard for this industry of 1,250 employees or less.[220] U.S. Census Bureau data for 2012 show that 841 establishments operated in this industry in that year.[221] Of that number, 828 establishments operated with fewer than 1,000 employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments

---

[213] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334290, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334290.

[214] U.S. Census Bureau, 2012 NAICS Definitions, "334210 Telephone Apparatus Manufacturing," https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.334210#.

[215] 13 CFR § 121.201, NAICS code 334210.

[216] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334210, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334210. The number of "establishments" is a less helpful indicator of small business prevalence in this context than would be the number of "firms" or "companies," because the latter take into account the concept of common ownership or control. Any single physical location for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census data for firms or companies only gives the total number of such entities for 2012, which was 250. *See also* https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG1//naics~334210.

[217] *Id*. An additional 4 establishments had employment of 2,500 or more.

[218] The NAICS Code for this service is 334220. 13 C.F.R 121.201. *See also* U.S. Census Bureau, 2012 NAICS Definitions, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing" https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.334220#.

[219] *Id*.

operated with 2,500 or more employees.[222] Based on this data, we conclude that a majority of manufacturers in this industry are small.

58. *Other Communications Equipment Manufacturing*. This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[223] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[224] The SBA has established a size for this industry as all such firms having 750 or fewer employees.[225] U.S. Census Bureau data for 2012 show that 383 establishments operated in that year.[226] Of that number 379 operated with fewer than 500 employees and 4 had 500 to 999 employees.[227] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

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

59. *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.[228] 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.[229] This restriction applies to any and all equipment and services, including software, produced or provided by a covered company.[230] Because the rule is prospective in effect, it does not prohibit the use of existing services or equipment already deployed or in use.[231] USF recipients may seek waivers of the requirements.[232]

60. *Covered Companies*. The Order initially designates Huawei and ZTE as covered

(Continued from previous page)

[220] 13 CFR § 121.201, NAICS Code 334220.

[221] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334220, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334220.

[222] *Id*.

[223] U.S. Census Bureau, 2017 NAICS Definitions, NAICS Code "334290 Other Communications Equipment Manufacturing"; https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334290&search=2017+NAICS+Search&search=2017.

[224] *Id*.

[225] 13 CFR § 121.201, NAICS code 334290.

[226] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334290, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334290.

[227] *Id*.

[228] *See supra Report and Order* at para. 26.

[229] *See supra Report and Order* at para. 66.

[230] *See id*.

[231] *See supra Report and Order* at para. 85.

[232] *See supra Report and Order* at para. 82.

companies for purposes of the prohibition we adopt today.[233] Independently, the Order establishes a process for designating entities as national security threats for purposes of our rule,[234] and delegates to the Public Safety and Homeland Security Bureau the authority to implement this process, as well as the next steps in the designation processes for Huawei and ZTE.[235] Because equipment from subsidiaries, parents, and affiliates pose the same risks to network integrity as equipment directly from the covered company, we include any subsidiary, parent, or affiliate of a covered company as a covered company subject to our prohibition.[236]

61. *Effective Date of Rule*. Because of the compelling interest in protecting our national security, we conclude that the rule we adopt today should take effect immediately upon publication in the Federal Register.[237] 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.[238] 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,[239] including approval by the Office of Management and Budget (OMB) under the Paperwork Reduction Act.[240] For E-Rate and Rural Health Care Recipients, the rule we adopt will apply to all funding years that start after the designation of a covered company.[241] Our 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 this rule.[242]

62. *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 the Wireline Competition Bureau, 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.[243]

63. *Audits and Recovery of Funds*. The Order directs USAC to implement audit procedures for each USF program consistent with the adopted rule.[244] 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.[245] 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

---

[233] *See supra Report and Order* at para. 43.

[234] *See supra Report and Order* at paras. 39-42.

[235] *See supra Report and Order* at paras. 64-65.

[236] *See supra Report and Order* at para. 39.

[237] *See supra Report and Order* at para. 83.

[238] *See id*.

[239] *See supra Report and Order* at para. 79.

[240] *See supra Report and Order* at para. 83.

[241] *See supra Report and Order* at para. 86.

[242] *See supra Report and Order* at para. 87.

[243] *See supra Report and Order* at para. 79.

[244] *See supra Report and Order* at para. 80.

[245] *See id*.

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.[246] To the extent that other ETCs do not yet report information to USAC that would verify compliance, we direct 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.[247] 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.[248]

64. *Information Collection*. The Information Collection Order directs the Wireline Competition Bureau and Office of Economics and Analytics, 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.[249] 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.[250] 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 our proposed rule (and among USF recipients the most likely to currently own and use equipment and services from Huawei and ZTE).[251] We therefore limit our information collection only to ETCs and will not require cost information from other USF recipients at this time.[252] We 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).[253] And we will allow other USF recipients who are not ETCs to participate on a voluntary basis as well.[254]

65. In implementing this 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.[255] ETCs must demonstrate how they arrived at any cost estimates they provide in response to this information collection. All submissions must be certified to ensure the accuracy of the responses.[256] This information collection shall be mandatory for all ETCs and voluntary for others.[257] This information collection applies to all subsidiaries and affiliates of ETCs.[258] 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

[246] *See id*.

[247] *See id*.

[248] *See supra Report and Order* at para. 81.

[249] *See supra Information Collection Order* at para. 162.

[250] *See supra Information Collection Order* at para. 163.

[251] *See supra Information Collection Order* at para. 164.

[252] *See id*.

[253] *See id*.

[254] *See id*.

[255] *See supra Information Collection Order* at para. 165.

[256] *See id*.

[257] *See supra Information Collection Order* at para. 166.

[258] *See supra Information Collection Order* at para. 163 n.380.

(e.g., granular location information).[259] We expect, 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.[260] As part of this information collection, we direct WCB and OEA to seek any information necessary to verify responses provided by ETCs to this information collection, including by requiring further information from respondents.[261] We direct WCB and OEA to proceed expeditiously with the information collection, including by seeking emergency PRA approval from OMB, if necessary and appropriate.[262]

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

66. 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.[263]

67. 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.[264] USF recipients may continue to use equipment or services provided or produced by covered companies obtained prior to the issuance of this rule, although they may not use USF funds to purchase, obtain, maintain, improve, modify, or otherwise support such equipment or services in any way.[265] 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.[266] The Order also permits USF recipients to seek a waiver of the requirements.[267] In these ways, the Order seeks to minimize the economic burden of these rules on small entities.

G. Report to Congress

68. The Commission will send a copy of the Report and Order and Information Collection Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[268] In addition, the Commission will send a copy of the Report and Order and Information Collection Order, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Report and Order, Information Collection Order, and FRFA (or summaries thereof) will also be published in the Federal Register.[269]

---

[259] *See supra Information Collection Order* at para. 166.

[260] *See id*.

[261] *See id*.

[262] *See id*.

[263] *See* 5 U.S.C. § 604(a)(6).

[264] *See supra Report and Order* at para. 85.

[265] *See id*.

[266] *See supra Report and Order* at para. 78.

[267] *See supra Report and Order* at para. 82.

[268] *See* 5 U.S.C. § 801(a)(1)(A).

[269] *See* 5 U.S.C. § 604(b).

APPENDIX D

Initial Regulatory Flexibility Analysis

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

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

2. Consistent with our obligation to be responsible stewards of the public funds used in the Universal Service Fund (USF) programs and increasing concern about ensuring communications supply chain integrity, the FNPRM proposes and seeks comment on a rule conditioning receipt of USF support on certification by an eligible telecommunications carrier (ETC) that it does not use covered equipment or services from companies that pose a national security threat to communications networks or the communications supply chain. The FNPRM also seeks comment on establishing a program for the funding of reasonable replacement costs for ETCs affected by the new condition on USF support.

B. Legal Basis

3. The proposed action is authorized under sections 1-4, 201(b), and 254 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201(b), and 254, and supported by section 889(b)(2)-(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[4]

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

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[5] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[6] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[7] A small business concern is one that: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the Small Business Administration (SBA).[8]

---

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

[2] *See* 5 U.S.C. § 603(a).

[3] *See id.*

[4] *2019 NDAA*, Sec. 889, 132 Stat. at 1917.

[5] 5 U.S.C. § 603(b)(3).

[6] 5 U.S.C. § 601(6).

[7] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small business concern" in 15 U.S.C. § 632). Pursuant to the RFA, the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register." 5 U.S.C. § 601(3).

[8] *See* 15 U.S.C. § 632.

5. *Small Businesses, Small Organizations, Small Governmental Jurisdictions*. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[9] 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.[10] These types of small businesses represent 99.9% of all businesses in the United States which translates to 28.8 million businesses.[11]

6. 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."[12] 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).[13]

7. 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."[14] U.S. Census Bureau data from the 2012 Census of Governments[15] indicates that there were 90,056 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[16] Of this number there were 37, 132 general purpose governments (county[17], municipal and town or township[18]) with populations of less than 50,000 and 12,184 special purpose governments (independent school districts[19] and special districts[20]) 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.[21] Based on this data we estimate that at least 49,316 local government

[9] *See* 5 U.S.C. § 601(3)-(6).

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

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

[12] 5 U.S.C. § 601(4).

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

[14] 5 U.S.C. § 601(5).

[15] *See* 13 U.S.C. § 161. The Census of Government is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Program Description, Census of Governments, https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=program&id=program.en.COG# .

jurisdictions fall in the category of "small governmental jurisdictions."[22]

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

1. Providers of Telecommunications and Other Services

a. Telecommunications Service Providers

9. *Incumbent Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers and under the SBA size standard, such a business is small if it has 1,500 or fewer employees.[23] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year. Of this total, 3,083 operated with fewer than 1,000 employees.[24] Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers.[25] Of this total, an estimated 1,006 have 1,500 or fewer employees.[26] Thus using the SBA's size standard the majority of Incumbent LECs can be considered small entities.

10. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to providers of interexchange services (IXCs). The closest NAICS Code category is Wired Telecommunications Carriers and the applicable size standard under SBA rules consists of all such companies having 1,500 or fewer employees.[27] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[28] Of that number, 3,083 operated with fewer than 1,000 employees.[29] According to internally developed Commission data, 359 companies

(Continued from previous page)

[16] *See* U.S. Census Bureau, 2012 Census of Governments, Local Governments by Type and State: 2012 - United States-States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG02.US01. Local governmental jurisdictions are classified in two categories - General purpose governments (county, municipal and town or township) and Special purpose governments (special districts and independent school districts).

[17] *See* U.S. Census Bureau, 2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01. There were 2,114 county governments with populations less than 50,000.

[18] *See* U.S. Census Bureau, 2012 Census of Governments, Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States – States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01. There were 18,811 municipal and 16,207 town and township governments with populations less than 50,000.

[19] *See* U.S. Census Bureau, *2012 Census of Governments, Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United States-States*. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01. There were 12,184 independent school districts with enrollment populations less than 50,000.

[20] *See* U.S. Census Bureau, *2012 Census of Governments, Special District Governments by Function and State: 2012 - United States-States*. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG09.US01. The U.S. Census Bureau data did not provide a population breakout for special district governments.

[21] *See* U.S. Census Bureau, *2012 Census of Governments, County Governments by Population-Size Group and State: 2012 - United States-States* - https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG06.US01; U.S. Census Bureau, American Factfinder, *Subcounty General-Purpose Governments by Population-Size Group and State: 2012 - United States–States* - https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG07.US01; and U.S. Census Bureau, *Elementary and Secondary School Systems by Enrollment-Size Group and State: 2012 - United*

(continued….)

reported that their primary telecommunications service activity was the provision of interexchange services.[30] Of this total, an estimated 317 have 1,500 or fewer employees.[31] Consequently, the Commission estimates that the majority of interexchange service providers that may be affected are small entities.

11. *Competitive Access Providers*. Neither the Commission nor the SBA has developed a definition of small entities specifically applicable to competitive access services providers (CAPs). The closest applicable definition under the SBA rules is Wired Telecommunications Carriers and under the size standard, such a business is small if it has 1,500 or fewer employees.[32] U.S. Census Bureau data for 2012 indicates that 3,117 firms operated during that year.[33] Of that number, 3,083 operated with fewer than 1,000 employees.[34] Consequently, the Commission estimates that most competitive access providers are small businesses that may be affected by our actions. According to Commission data the *2010 Trends in Telephone Report*, 1,442 CAPs and competitive local exchange carriers (competitive LECs) reported that they were engaged in the provision of competitive local exchange services.[35] Of these 1,442 CAPs and competitive LECs, an estimated 1,256 have 1,500 or fewer employees and 186 have more than 1,500 employees.[36] Consequently, the Commission estimates that most providers of competitive exchange services are small businesses.

12. *Operator Service Providers (OSPs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for operator service providers. The appropriate category for Operator Service Providers is the category Wired Telecommunications Carriers. Under that size standard, such a business is small if it has 1,500 or fewer employees.[37] Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[38] Thus, under this size standard, the majority of firms in this industry can be considered small. According to Commission data, 33 carriers have reported that they are engaged in the provision of operator services. [39] Of these, an estimated 31 have 1,500 or fewer employees and two have more than 1,500 employees.[40] Consequently, the Commission estimates that the majority of OSPs are small entities

(Continued from previous page)
States-States. https://factfinder.census.gov/bkmk/table/1.0/en/COG/2012/ORG11.US01. While U.S. Census Bureau data did not provide a population breakout for special district governments, if the population of less than 50,000 for this category of local government is consistent with the other types of local governments the majority of the 38, 266 special district governments have populations of less than 50,000.

[22] *Id.*

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

[24] *Id*.

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

[26] *Id*.

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

[28] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[29] *Id*.

that may be affected by the rules proposed.

13. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.[41] Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees.[42] Census Bureau data from 2012 show that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees.[43] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services.[44] Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees.[45] Consequently, the Commission estimates that the majority of local resellers are small entities that may be affected by the rules adopted.

14. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry.[46] The SBA has developed a small business size standard for the category of Telecommunications Resellers.[47] Under that size standard, such a business is small if it has 1,500 or fewer employees.[48] 2012 Census Bureau data show that 1,341 firms provided resale services during that

(Continued from previous page)

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

[31] *Id.*

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

[33] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[34] *Id.*

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

[36] *Id.*

[37] 13 CFR § 121.201. The Wired Telecommunications Carrier category formerly used the NAICS code of 517110. As of 2017 the U.S. Census Bureau definition shows the NAICs code as 517311 for Wired Telecommunications Carriers. *See* https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[38] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Information: Subject Series - Estab & Firm Size: Receipts Size of Firms for the U.S.: 2012, http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

[39] *Trends in Telephone Service*, tbl. 5.3.

year. Of that number, 1,341 operated with fewer than 1,000 employees.[49] Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services.[50] Of this total, an estimated 857 have 1,500 or fewer employees.[51] Consequently, the Commission estimates that the majority of toll resellers are small entities.

15. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry."[52] The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees.[53] U.S. Census data for 2012 show that there were 3,117 firms that operated that year.[54] Of this total, 3,083 operated with fewer than 1,000 employees.[55] Thus, under this size standard, the majority of firms in this industry can be considered small.

16. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[56] The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees.[57] For this industry, U.S. Census Bureau data for 2012 show that there

(Continued from previous page)

[40] *Id.*

[41] U.S. Census Bureau, 2017 NAICS Definition, 517911 Telecommunications Resellers, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

[42] 13 CFR § 121.201, NAICS code 517911.

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

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

[45] *See id*.

[46] U.S. Census Bureau, 2017 NAICS Definition, 517911 Telecommunications Resellers, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517911&search=2017%20NAICS%20Search.

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

[48] *Id.*

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

[50] *Trends in Telephone Service* at tbl. 5.3.

[51] *Id.*

[52] *See* 13 CFR § 120.201. The Wired Telecommunications Carrier category formerly used the NAICS code of 517110. As of 2017 the U.S. Census Bureau definition shows the NAICS code as 517311 for Wired

(continued….)

were 967 firms that operated for the entire year.[58] Of this total, 955 firms had employment of 999 or fewer employees and 12 had employment of 1000 employees or more.[59] Thus under this category and the associated size standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

17. The Commission's own data—available in its Universal Licensing System—indicate that, as of October 25, 2016, there are 280 Cellular licensees that will be affected by our actions today.[60] The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services.[61] Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees.[62] Thus, using available data, we estimate that the majority of wireless firms can be considered small.

18. *Common Carrier Paging.* As noted, since 2007 the Census Bureau has placed paging providers within the broad economic census category of Wireless Telecommunications Carriers (except Satellite).[63]

19. In addition, in the *Paging Second Report and Order*, the Commission adopted a size standard for "small businesses" for purposes of determining their eligibility for special provisions such as bidding credits and installment payments.[64] A small business is an entity that, together with its affiliates and controlling principals, has average gross revenues not exceeding $15 million for the preceding three years.[65] The SBA has approved this definition.[66] An initial auction of Metropolitan Economic Area ("MEA") licenses was conducted in the year 2000. Of the 2,499 licenses auctioned, 985 were sold.[67] Fifty-seven companies claiming small business status won 440 licenses.[68] A subsequent auction of MEA and Economic Area ("EA") licenses was held in the year 2001. Of the 15,514 licenses auctioned, 5,323

(Continued from previous page)
Telecommunications Carriers. *See*, https://www.census.gov/cgi-bin/sssd/naics/naicsrch?code=517311&search=2017.

[53] *Id*.

[54] *See* U.S. Census Bureau, *2012 Economic Census of the United States,* Table No. EC1251SSSZ5, *Information: Subject Series - Estab & Firm Size: Employment Size of Firms: 2012* (517110 Wired Telecommunications Carriers). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517110.

[55] *Id.*

[56] NAICS Code 517210. *See* https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.517210.

[57] 13 CFR § 121.201, NAICS code 517210.

[58] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ5, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012 NAICS Code 517210 (rel. Jan. 8, 2016). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517210.

[59] *Id*. Available census data does not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with "1000 employees or more."

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

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

[62] *See id*.

were sold.[69] One hundred thirty-two companies claiming small business status purchased 3,724 licenses. A third auction, consisting of 8,874 licenses in each of 175 EAs and 1,328 licenses in all but three of the 51 MEAs, was held in 2003. Seventy-seven bidders claiming small or very small business status won 2,093 licenses.[70]

20. Currently, there are approximately 74,000 Common Carrier Paging licenses. According to the most recent Trends in Telephone Service, 291 carriers reported that they were engaged in the provision of "paging and messaging" services.[71] Of these, an estimated 289 have 1,500 or fewer employees and two have more than 1,500 employees.[72] We estimate that the majority of common carrier paging providers would qualify as small entities under the SBA definition.

21. *Wireless Telephony*. Wireless telephony includes cellular, personal communications services, and specialized mobile radio telephony carriers. The closest applicable SBA category is Wireless Telecommunications Carriers (except Satellite)[73] and the appropriate size standard for this category under the SBA rules is that such a business is small if it has 1,500 or fewer employees.[74] For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year.[75] Of this total, 955 firms had fewer than 1,000 employees and 12 firms has 1000 employees or more.[76] Thus under this category and the associated size standard, the Commission estimates that a majority of these entities can be considered small. According to Commission data, 413 carriers reported that they were engaged in wireless telephony.[77] Of these, an estimated 261 have 1,500 or fewer employees and 152 have more than 1,500 employees.[78] Therefore, more than half of these entities can be considered small.

22. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or

(Continued from previous page)

[63] *See* U.S. Census Bureau, 2007 NAICS Definitions, "517210 Wireless Telecommunications Categories (Except Satellite)", http://www.census.gov/naics/2007/def/ND517210.HTM#N517210 (last visited Oct. 24, 2017).

[64] *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems et al.*, WT Docket No. 96-18 et al., Second Report and Order and Further Notice of Proposed Rulemaking, 12 FCC Rcd 2732, 2811-12, paras. 178-81 (1997) (*Paging Second Report and Order*); *Revision of Part 22 and Part 90 of the Commission's Rules to Facilitate Future Development of Paging Systems et al.*, Memorandum Opinion and Order on Reconsideration and Third Report and Order, 14 FCC Rcd 10030, 10085-88, paras. 98-107 (1999).

[65] *Paging Second Report and Order*, 12 FCC Rcd at 2811, para. 179.

[66] *See* Letter from Aida Alvarez, Administrator, SBA, to Amy Zoslov, Chief, Auctions and Industry Analysis Division, Wireless Telecommunications Bureau, FCC (Dec. 2, 1998).

[67] *See 929 and 931 MHz Paging Auction Closes*, Public Notice, 15 FCC Rcd 4858 (WTB 2000).

[68] *See id.*

[69] *See Lower and Upper Paging Bands Auction Closes*, Public Notice, 16 FCC Rcd 21821 (WTB 2001).

[70] *See Lower and Upper Paging Bands Auction Closes*, Public Notice, 18 FCC Rcd 11154 (WTB 2003). The current number of small or very small business entities that hold wireless licenses may differ significantly from the number of such entities that won in spectrum auctions due to assignments and transfers of licenses in the secondary market over time. In addition, some of the same small business entities may have won licenses in more than one auction.

[71] *2010 Trends Report* at Table 5.3, page 5-5.

[72] *Id*.

[73] 13 CFR § 121.201, NAICS code 517210.

reselling satellite telecommunications."[79] Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $32.5 million or less in average annual receipts, under SBA rules.[80] For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year.[81] Of this total, 299 firms had annual receipts of less than $25 million.[82] Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

23. *All Other Telecommunications*. The "All Other Telecommunications" category is comprised of establishments that are primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[83] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[84] Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry.[85] The SBA has developed a small business size standard for "All Other Telecommunications," which consists of all such firms with gross annual receipts of $32.5 million or less.[86] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year.[87] Of these firms, a total of 1,400 had gross annual receipts of less than $25 million and 42 firms had gross annual receipts of $25 million to $49, 999,999.[88] Thus, the Commission estimates that a majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

b. Internet Service Providers

24. *Internet Service Providers (Broadband)*. Broadband Internet service providers include wired (e.g., cable, DSL) and VoIP service providers using their own operated wired telecommunications

(Continued from previous page)

[74] *Id*.

[75] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ5, Information: Subject Series: Estab and Firm Size: Employment Size of Firms for the U.S.: 2012 NAICS Code 517210 (rel. Jan. 8, 2016). https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ5//naics~517210.

[76] *Id*. Available census data do not provide a more precise estimate of the number of firms that have employment of 1,500 or fewer employees; the largest category provided is for firms with "1000 employees or more."

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

[78] *Id*.

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

[80] 13 CFR § 121.201, NAICS code 517410.

[81] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517410 https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ4//naics~517410.

[82] *Id*.

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

[84] *Id*.

[85] *Id*.

infrastructure fall in the category of Wired Telecommunication Carriers.[89] Wired Telecommunications Carriers are comprised of establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies.[90] The SBA size standard for this category classifies a business as small if it has 1,500 or fewer employees.[91] U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees.[92] Consequently, under this size standard the majority of firms in this industry can be considered small.

25. *Internet Service Providers (Non-Broadband).* Internet access service providers such as Dial-up Internet service providers, VoIP service providers using client-supplied telecommunications connections and Internet service providers using client-supplied telecommunications connections (e.g., dial-up ISPs) fall in the category of All Other Telecommunications. The SBA has developed a small business size standard for All Other Telecommunications which consists of all such firms with gross annual receipts of $32.5 million or less.[93] For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year. Of these firms, a total of 1,400 had gross annual receipts of less than $25 million.[94] Consequently, under this size standard a majority of firms in this industry can be considered small.

c. Vendors and Equipment Manufacturers

26. *Vendors of Infrastructure Development or "Network Buildout."* The Commission has not developed a small business size standard specifically directed toward manufacturers of network facilities. There are two applicable SBA categories in which manufacturers of network facilities could fall and each have different size standards under the SBA rules. The SBA categories are "Radio and Television Broadcasting and Wireless Communications Equipment" with a size standard of 1,250 employees or less[95] and "Other Communications Equipment Manufacturing" with a size standard of 750

(Continued from previous page)

[86] 13 CFR § 121.201; NAICS Code 517919.

[87] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab and Firm Size: Receipts Size of Firms for the United States: 2012, NAICS code 517919, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/51SSSZ4//naics~517919.

[88] *Id.*

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

[90] *Id.*

[91] *Id.*

[92] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size, NAICS code 334290, http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ2&prodType=table.

[93] 13 CFR § 121.201; NAICS Code 517919.

[94] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1251SSSZ4, Information: Subject Series - Estab & Firm Size: Receipts Size of Firms for the U.S.: 2012, NAICS Code 517919, https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ECN_2012_US_51SSSZ4&prodType=table.

[95] 13 CFR § 121.201, NAICS Code 334220.

employees or less."[96] U.S. Census Bureau data for 2012 show that for Radio and Television Broadcasting and Wireless Communications Equipment firms 841 establishments operated for the entire year.[97] Of that number, 828 establishments operated with fewer than 1,000 employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments operated with 2,500 or more employees.[98] For Other Communications Equipment Manufacturing, U.S. Census Bureau data for 2012 show that 383 establishments operated for the year.[99] Of that number 379 firms operated with fewer than 500 employees and 4 had 500 to 999 employees. Based on this data, we conclude that the majority of Vendors of Infrastructure Development or "Network Buildout" are small.

27. *Telephone Apparatus Manufacturing*. This industry comprises establishments primarily engaged in manufacturing wire telephone and data communications equipment. These products may be standalone or board-level components of a larger system. Examples of products made by these establishments are central office switching equipment, cordless telephones (except cellular), PBX equipment, telephones, telephone answering machines, LAN modems, multi-user modems, and other data communications equipment, such as bridges, routers, and gateways."[100] The SBA size standard for Telephone Apparatus Manufacturing is all such firms having 1,250 or fewer employees.[101] According to U.S. Census Bureau data for 2012, there were a total of 266 establishments in this category that operated for the entire year.[102] Of this total, 262 had employment of under 1,000, and an additional 4 had employment of 1,000 to 2,499.[103] Thus, under this size standard, the majority of firms can be considered small.

28. *Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing.* This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[104] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and

---

[96] 13 CFR § 121.201, NAICS Code 334290.

[97] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334220, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334220.

[98] *Id*.

[99] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334290, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334290.

[100] U.S. Census Bureau, 2012 NAICS Definitions, "334210 Telephone Apparatus Manufacturing," https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.334210#.

[101] 13 CFR § 121.201, NAICS code 334210.

[102] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334210, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334210. The number of "establishments" is a less helpful indicator of small business prevalence in this context than would be the number of "firms" or "companies," because the latter take into account the concept of common ownership or control. Any single physical location for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census data for firms or companies only gives the total number of such entities for 2012, which was 250. *See also* https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG1//naics~334210.

broadcasting equipment.[105] The SBA has established a small business size standard for this industry of 1,250 employees or less.[106] U.S. Census Bureau data for 2012 show that 841 establishments operated in this industry in that year.[107] Of that number, 828 establishments operated with fewer than 1,000 employees, 7 establishments operated with between 1,000 and 2,499 employees and 6 establishments operated with 2,500 or more employees.[108] Based on this data, we conclude that a majority of manufacturers in this industry are small.

29. *Other Communications Equipment Manufacturing.* This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[109] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[110] The SBA has established a size for this industry as all such firms having 750 or fewer employees.[111] U.S. Census Bureau data for 2012 show that 383 establishments operated in that year.[112] Of that number 379 operated with fewer than 500 employees and 4 had 500 to 999 employees.[113] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

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

30. The FNPRM proposes a rule that conditions universal service support on a certification that ETCs are not using 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. We seek comment on this proposal, and its likely costs and benefits, as well as on alternative approaches and any other steps we should consider taking. The FNPRM also seeks comment on how broadly this proposed rule should apply, and how it should be implemented. We seek comment on how to enforce the proposed rule, including who should be held liable for the recovery of disbursed funds. We also seek comment on establishing a program for the funding of reasonable replacement costs for ETCs affected by

(Continued from previous page)

[103] *Id*. An additional 4 establishments had employment of 2,500 or more.

[104] The NAICS Code for this service is 334220. 13 C.F.R 121.201. *See also* U.S. Census Bureau, 2012 NAICS Definitions, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing" https://factfinder.census.gov/faces/affhelp/jsf/pages/metadata.xhtml?lang=en&type=ib&id=ib.en./ECN.NAICS2012.334220#.

[105] *Id*.

[106] 13 CFR § 121.201, NAICS Code 334220.

[107] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334220, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334220.

[108] *Id*.

[109] U.S. Census Bureau, 2017 NAICS Definitions, NAICS Code "334290 Other Communications Equipment Manufacturing"; https://www.census.gov/cgi-bin/sssd/naics/naicsrch?input=334290&search=2017+NAICS+Search&search=2017.

[110] *Id.*

[111] 13 CFR § 121.201, NAICS code 334290.

[112] U.S. Census Bureau, *2012 Economic Census of the United States*, Table EC1231SG2, Manufacturing: Summary Series: General Summary: Industry Statistics for Subsectors and Industries by Employment Size: 2012, NAICS Code 334290, https://factfinder.census.gov/bkmk/table/1.0/en/ECN/2012_US/31SG2//naics~334290.

[113] *Id.*

the new condition on USF support. Lastly, we seek comment on whether sections 201(b) and 254 provide legal authority for the proposed rule.[114]

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

31. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[115]

32. In compliance with the direction to the Commission provided in the 2019 NDAA, the FNPRM specifically proposes to establish a funding mechanism to reimburse entities, particularly small and rural carriers, for the costs of replacing the covered equipment. The FNPRM also seeks comment on whether there are any compliance issues we should consider, particularly for smaller carriers.

33. We expect to take into account the economic impact on small entities, as identified in comments filed in response to the FNPRM and this IRFA, in reaching our final conclusions and promulgating rules in this proceeding. In addition to taking into the account the size of the entity in potentially establishing transition periods to come into compliance with the proposed condition on future USF support, we also seek comment on establishing a program for the funding of reasonable replacement costs for ETCs affected by the new condition on USF support, which would include small ETCs.

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

34. None.

[114] *See* 5 U.S.C. § 254.

[115] *See* 5 U.S.C. § 603(c).

APPENDIX E

Classified Supplement

STATEMENT OF
CHAIRMAN AJIT PAI

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

Last year, testifying before Congress, FBI Director Chris Wray said, "[W]e're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks that provides the capacity to exert pressure or control over our telecommunications infrastructure."[1]

And last week, Attorney General Bill Barr wrote to us:

> [W]e are at a critical moment of technological change. Telecommunications providers in America and around the world are deciding who should build and service the Fifth Generation (5G) of wireless networks. We will become even more dependent on those networks as more and more devices and services are connected and operate at unprecedented speeds. Human life and safety as well as critical government functions will ride on them. Our national defense will depend on the security of our allies' networks as well as our own. Protecting our networks (rural and urban alike) from equipment or services offered by companies posing a threat to the integrity of those networks is therefore a vital national security goal.[2]

At the FCC, we couldn't agree more with the Attorney General and the Director of the FBI. That's why today, we adopt a ban on using funds from the FCC's Universal Service Fund (USF) equipment or services from companies posing a national security threat to the integrity of communications networks or the communications supply chain. We also initially designate two Chinese companies—Huawei and ZTE—as "covered" companies for purposes of this rule, and we set up a process for designating additional such companies in the future.

We take these actions based on evidence in the record as well as longstanding concerns from the executive and legislative branches about the national security threats posed by certain foreign communications equipment manufacturers, most particularly Huawei and ZTE. Both companies have close ties to China's Communist government and military apparatus. Both companies are subject to Chinese laws broadly obligating them to cooperate with any request from the country's intelligence services and to keep those requests secret. Both companies have engaged in conduct like intellectual property theft, bribery, and corruption.

Moreover, we know that hidden "backdoors" to our networks in routers, switches, and other network equipment can allow a hostile adversary to inject viruses and other malware, steal Americans' private data, spy on U.S. companies, and more. Indeed, just last month, the European Union found 5G security risks where a "hostile state actor exercises pressure over a supplier under its jurisdiction to provide access to sensitive network assets through (either purposefully or unintentionally) embedded vulnerabilities."[3]

---

[1] Hearing before the Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community," 115th Cong. (Feb. 13, 2018) (statement of Christopher Wray, Director, FBI), https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#.

[2] Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, FCC, WC Docket No. 18-89, at 1 (Nov. 13, 2019), https://ecfsapi.fcc.gov/file/111501201939/18-89A.pdf.

[3] European Union, "EU coordinated risk assessment of the cybersecurity of 5G networks" at 27 (Oct. 2019), https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

These concerns are by no means hypothetical. This summer, for example, an independent cybersecurity firm found that over half of the Huawei firmware images they analyzed had at least one potential backdoor and that each Huawei device they tested had an average of 102 known vulnerabilities.[4] Similarly, in March 2019, an oversight board in the United Kingdom released a report identifying "[f]urther significant technical issues . . . in Huawei's engineering processes, leading to new risks in the UK telecommunications networks."[5] It also said that it "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."[6] It is unsurprising, then, that in the last 12 months, three of our closest allies—New Zealand, Japan, and Australia—have issued bans on Huawei equipment and that over 30 nations (including the U.S.) have embraced a risk-based framework called the Prague Proposals.[7]

Given the threats posed by Huawei and ZTE to America's security and our 5G future, this FCC will not sit idly by and hope for the best. Today, we not only ensure that the federal funds in the USF are not spent on equipment or services from these suppliers, but we also propose a process to remove such equipment already deployed in USF-funded networks. Specifically, we propose to require certain carriers receiving USF funds, known as eligible telecommunications carriers, to remove from their networks existing equipment from covered companies, starting with Huawei and ZTE. To mitigate the financial impact of this requirement, particularly on small, rural carriers, we propose to establish a reimbursement program to help offset the cost of transitioning to more trusted vendors.

Finally, to aid the design of a removal and replacement program, we require carriers to submit information on their use of equipment from Huawei and ZTE as well as the potential costs associated with removal and replacement of such equipment.

In taking these steps, we demonstrate the FCC's commitment to doing everything we can within our statutory authority to address national security threats to our communications networks, and together with our federal partners, to secure our 5G future.

For their outstanding work on this item, I'd like to thank Callie Coker, Kate Dumouchel, Justin Faulb, Ellen Gardiner, Aaron Garza, Trent Harkrader, Billy Layton, Kris Monteith, Ryan Palmer, Gilbert Smith, Cody Venzke, and John Visclosky of the Wireline Competition Bureau; Kenneth Baker, Erin Boone, Garnet Hanley, Kari Hicks, Charles Mathias, Dana Shaffer, Sean Spivey, Donald Stockdale, Joel Taubenblatt, and Suzanne Tetreault of the Wireless Telecommunications Bureau; Steven Carpenter, Michael Connelly, Lisa Fowlkes, Jeffrey Goldthorp, Kurian Jacobs, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Saswat Misra, and Austin Randazzo of the Public Safety and Homeland Security Bureau; Denise Coca, Kathleen Collins, Gabrielle Kim, David Krech, Arthur Lechtman, Thomas Sullivan, and Troy Tanner of the International Bureau; Rosemary Harold, Christopher Killion, Shannon Lipp, and Jeremy Marcus of the Enforcement Bureau; Ira Keltz, Julius Knapp, Aspasia Paroutsas, and Ronald Repasi of the Office of Engineering and Technology; Malena Barzilai, Michael Carlson, Thomas Johnson, Douglas Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel; Maura McGowan and Sanford Williams of the Office of Communications Business

---

[4] "Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd." at 3 (June 2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf.

[5] "Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board Annual Report 2019: A report to the National Security Adviser of the United Kingdom" at 2 (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[6] *Id.* at 3.

[7] *See* "Prague 5G Security Conference announced series of recommendations: The Prague Proposals" (May 3, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Opportunities; and Eric Burger, Octavian Carare, Jim Eisner, Kenneth Lynch, Alec MacDonnell, Giulia McHenry, Chuck Needy, Eric Ralph, Steven Rosenberg, Craig Stroup, Emily Talaga, and Geoff Waldau of the Office of Economics and Analytics.

STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY

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

Communications networks – whether wired or wireless, fixed or mobile, existing or yet to be deployed – are, and will continue to be, a central component of our daily lives. They no longer are just a means to talk to our friends and family, but facilitate how we conduct business, make financial transactions, engage in commerce, and obtain needed information. This will only expand in the coming years as next-generation networks could bring about such advances as self-driving vehicles, remote surgery and other telehealth applications, and the Internet of Things, with billions upon billions of devices conveying information through the Internet. While we do not fully know all of the innovative applications that are on the horizon, it is possible to conclude that a huge amount of data, including very sensitive information, will be traveling through these networks. Therefore, they must be as secure as possible, knowing that absolute security is unachievable, and we must ensure that those with nefarious intentions cannot get access to these systems – or the information they carry – to do harm to our country.

I have spoken on many occasions about the threats to our networks by those countries and their associated businesses that do not share our market-based system or support our values and freedoms. We see time and time again efforts by these entities to attempt to monopolize and gain unfair advantages in the marketplace. Further, I agree that the hard-earned dollars of the American people should not be used to buy equipment and support entities that may do us harm.

For a multitude of reasons, I support today's item. But, I do have a few reservations. Let me caution the critics: raising concerns on certain portions doesn't make me a sympathizer of those seeking to harm the U.S. I am just trying to enact sound policy and prevent potential abuses down the round. Being skeptical of and trying to protect from an authoritative government is the very nature of being American.

First, I understand the gravity of the decision to exclude certain companies from the U.S. marketplace. These designated companies stand to lose significant business opportunities. Of course, I am not concerned about financial opportunities lost by companies that want to cause us harm, but sometimes innocent companies can be implicated by mistake. We must get these decisions right and have a process to challenge if the Bureau, which I am not all that comfortable delegating to, gets them wrong. I appreciate that the Chairman accommodated my concerns by implementing a 120-day timeline to expedite appeals of Bureau-level decisions to the Commission. This will ensure that affected parties have some timely recourse, if necessary.

Second, I fear that we are underestimating the costs of our action today. I was one of the first to suggest that our actions to ban certain equipment would have costs to be paid by someone, and I was criticized for doing so; now it is universally accepted. On this point, while I appreciate that the Chairman's Office and staff clarified how and when USF funds can be used when a network contains covered equipment, our decision to prohibit the use of USF funds to maintain, modify, or support covered equipment in any way may result in some providers having to replace equipment earlier than scheduled when minor changes or repairs need to be made. Not to mention that our communications providers will have fewer equipment options, which could raise costs and delay new and expanded offerings. Unfortunately, these costs will mostly affect the nation's smaller providers, which are more likely to have covered equipment and may be relying on USF dollars to remain viable.

More generally, I remain disappointed in our cost-benefit analyses. Instead of figuring out what the true benefits are of our decision, the cost-benefit analysis states that the cost of $960 million, which as I just stated seems low, is justified if our action prevents a minimal – well less than one percent – disruption to the economy and annual growth. There is no data provided to verify these assertions or

support the theory that preventing USF funds from being used to buy and maintain this equipment will be effective in reducing these hypothetical disruptions to our economy.

Third, I am concerned that we are broadly and unnecessarily interpreting some statutory provisions to justify our authority to decide that some companies should not be able to participate in our communications economy. While I am a fervent supporter of protecting our national security, these and similar arguments are likely to be used in the future to justify mandates in the name of national security or others. It is important to note that the Commission doesn't retain significant authority – or much at all – to affirmatively act on network security issues. That means we cannot transcribe requirements, mandates, or other burdens on providers in the name of network security. The "national security" language of the statute is not a catch-all, otherwise it can be abused in many harmful ways. However, we do have and rightfully maintain authorization authority where we take Team Telecom views into account and can condition USF in various ways to meet our policy objectives.

Regardless of these concerns about the item, I remain seriously concerned about the risks that our nation's communications networks face. I appreciate the Chairman's effort and thank him and Commission staff for tackling a very complex and challenging issue. I approve.

STATEMENT OF
COMMISSIONER BRENDAN CARR

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

Earlier this year, I had the privilege of visiting Malmstrom Air Force Base near Great Falls, Montana. I spent time there with Colonel Jennifer Reeves who is Commander of the 341st Missile Wing. Colonel Reeves and her team have one of the most significant and weighty missions in government. In their charge are150 intercontinental ballistic missiles loaded in underground silos spread across northern Montana. These are missiles that when launched can carry nuclear warheads almost 10,000 miles. Colonel Reeves told me that her job is to make sure they're always ready to go. Set against that destructive power is a completely serene and wide-open landscape—it's just wheat fields and Big Sky Country. Except as it turns out, there are cell towers all around the Montana missile fields running on Huawei equipment.[1] I got a firsthand look at those when I was up there.

This is not just a concern for the military. Everything we do in modern society now runs on interconnected networks, from banking, to transportation, and even our power grids. This will become only more so as carriers continue to build out 5G networks. If these networks are threatened, everything we have come to rely on is threatened. We have acknowledged the threat that Chinese telecom firms pose to our networks for some time. In 2012, the House Permanent Select Committee on Intelligence issued a report recommending that companies avoid using Huawei and ZTE equipment, and that government agencies remain vigilant and focused on the threat. Last year's National Defense Authorization Act prohibited government agencies and contractors from using Chinese equipment. The Department of Commerce has clamped down on the Chinese firms' abilities to do business with U.S. firms. Last year, we launched this proceeding to do our part to ensure U.S. national security. And this month Attorney General William P. Barr wrote to the Commission that, "we should not signal that Huawei and ZTE are anything other than a threat to our collective security."

When combined with the ever increasing sophistication of cyber attacks and the fact that attacks from state actors are by far the most well-funded and advanced, it's not hard to see the threat that companies like Huawei and ZTE pose to our networks and to our national security. Indeed, China's National Intelligence Law requires that all "organizations…cooperate with the State intelligence work," and it provides them no right to refuse.[2] It also gives the Chinese government the power to take over a company's communications equipment.[3] And because the networks in the U.S—from rural America to big city—are interconnected, even a small amount of compromised equipment could be devastating to U.S. security.

At the FCC, we are in a position to do something about this threat. And we are. Today, we are prohibiting carriers from using federal dollars to purchase any equipment or services from companies that pose a national security threat, including Huawei and ZTE.

And we are not stopping there. In 2018, I called on the FCC to expand our proceeding and put even more options on the table, including the removal of covered equipment that carriers have already installed in their networks. That would include some of the equipment I saw out in Montana. After all, if equipment poses a threat, it's not enough to stop subsidizing it: it must come out of the network. I am glad that we are moving forward with that idea and proposing to take that action today.

---

[1] Alex Marquardt and Michael Conte, *Huawei Connects rural America. Could it threaten the country's most sensitive military sites?* CNN, (Mar. 11, 2019) https://www.cnn.com/2019/03/11/politics/huawei-cell-towers-missile-silos/index.html.

[2] Chinese National Intelligence Law, Article 7.

[3] Chinese National Intelligence Law, Article 17.

I also want to thank my colleagues for agreeing to expand the scope of today's Further Notice. We now go beyond the initial proposal, which focused on removing equipment if the carrier receives federal support, to asking whether we should mandate the removal of covered equipment regardless of whether the communications provider receives federal support. I appreciate that my colleagues not only supported that suggestion but called for similar edits.

Today, the U.S. has the leading 5G networks in the world. And today's decision will help extend American leadership by ensuring the security of these vital networks.

I want to thank the staff of the Wireline Competition Bureau for their work on this item. It has my full support.

STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL

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

Picture central Montana. It's vast. There are plains as far as the eye can see. This is, after all, Big Sky country. In this wide-open area you'll find mostly wheat and cattle farms. But if you wander you're likely to happen upon Malmstrom Air Force Base. It's the home of the 341st Missile Wing of the Air Force Global Strike Command. On the outskirts of this Air Force Base, you'll find silos with more than 100 intercontinental ballistic missiles. As CNN has reported, they "stand at the ready, buried deep underground." These rockets can deliver nuclear warheads across the ocean thousands of miles away. They are an important part of the United States Strategic Command.

Next to those silos are something a lot more familiar to the Federal Communications Commission. There are clusters of cell phone towers that are operated by a small rural wireless carrier. You might not know it just by looking at them but these towers may represent a bigger risk to our national security than the missiles they surround. That's because the communications equipment that hangs on these towers is from Huawei, and we have good reason to believe it is susceptible to undue foreign influence and control.

Here's the thing. We have long known the risks of deployments that feature equipment developed by vendors like Huawei and ZTE. In fact, the federal government and our four nationwide carriers have shunned this technology because of its security vulnerabilities. But a number of small wireless carriers—serving remote areas like central Montana—have not. After all, Chinese-developed equipment is less costly to deploy and the economics of serving less populated rural communities are hard. So in some cases these insecure networks offer the only option for commercial wireless service in and around sensitive United States military bases in rural parts of the country.

It gets worse. This insecure equipment has been subsidized by the United States government and this very agency. It was purchased with money from the universal service fund at the FCC. If a foreign government ever chose to exploit the radio transmitters that have been placed alongside key military installations, it could suck up sensitive data, shut down service, or launch denial of service attacks. And it gets still worse, because as we transition to next-generation 5G networks, insecure equipment in the telecommunications supply chain could take cybersecurity risks to entirely new levels. That's because 5G networks will allow us to move and access vastly higher quantities of data, and we will depend on them more than prior technologies for a range of mission-critical applications.

This is just one military base in Montana. But there are others like it. Just as there all kinds of essential infrastructure across our rural communities and in many cases nestled nearby are wireless networks with insecure foreign equipment.

We need to do something about it. That's why eighteen months ago we started a rulemaking at the FCC aimed at fixing this problem. Today we take a long overdue first step to do just that. I have only one complaint with this effort: that it took us so long to get here. This is not hard. *It should not have taken us eighteen months to reach the conclusion that federal funds should not be used to purchase equipment that undermines national security.*

I support this effort. I also appreciate that my colleagues were willing to consider changes I offered to the decision and rulemaking we adopt today. In critical part, those include exploring our authority over carriers under the Communications Assistance for Law Enforcement Act to expand our prohibition beyond just the universal service program; providing additional guidance to companies so that our rules do not needlessly disrupt day-to-day service and operations in rural America; implementing the lessons learned from the 600 MHz incentive auction in order to maximize funds available for replacing insecure equipment; and seeking to accelerate the FCC's review of a reimbursement program.

So while I approve today's decision and rulemaking, I think the FCC has more work to do when it comes to network security. Because our present efforts to remove and replace insecure equipment are not bold enough. *We need a coordinated, national plan for managing the future of 5G security—and the evidence all around us makes crystal clear we don't have one.*

When the United States government pursues action against Huawei or ZTE, its objective should be security. But in Washington right now, I fear these issues can easily get swept up into broader trade matters. Despite our actions today, we have to grapple with the fact that at any moment the Administration could trade away our security objectives for some momentary advantage in bilateral trade negotiations. I hope that does not occur, but let's be honest, it has happened before, when this Administration reversed course on banning ZTE from doing business in the United States. If it happens again, it will have serious consequences for our credibility.

There is also a conspicuous lack of progress in other parts of the government tasked with addressing this set of problems. New supply chain rules from the Department of Commerce that were due last month reportedly have been derailed by interagency disputes. The Bureau of Industry and Security has extended three times—and as recently as just this week—the general license authority for United States companies to continue to work with the very companies the FCC is today trying to remove from our networks. On top of this, the national spectrum policy that was announced in last year's Executive Order has fallen by the wayside. It was due in July but is nowhere to be found. And the Administration's tariffs are making it harder for United States companies to invest because by adding up to a 25 percent fee on modems, antennas, and semiconductors it is driving up the cost of 5G deployment.

This does not inspire confidence. It's not a national plan for action. It's the right hand not talking to the left with consequences that are broader than Washington—they go directly to heart of our competitiveness in the global economy.

Nor has this gone unnoticed. Last week, *The Wall Street Journal* documented all the ways the federal government is tripping over itself in its efforts to support the roll out of 5G. This week, the bipartisan leadership of the Senate Select Committee on Intelligence, Committee on Homeland Security and Government Affairs, Foreign Relations Committee, and the Armed Services Committee wrote the White House expressing concern that we do not have a coordinated national strategy in place for 5G—and we need one. I agree.

Looking ahead, I have some ideas about just what a national strategy should include. Here are three to start.

First, we need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far because no network stands by itself. Our networks still will connect to insecure equipment abroad. So we need to begin researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to virtualize and diversify key parts of our networks.

I put forward an idea at Mobile World Congress last month to start this conversation. I suggested the FCC should explore opportunities to support improved security though open radio access networks—or what is known as open RAN. The RAN sits between your device and the core of the carrier network. It is the most expensive and restrictive part of the network today. All major components of a RAN have to come from the same vendor. There is no way to mix and match. But if we can unlock the RAN by virtualizing this component of the network with software and off the shelf hardware, we will increase network diversity and improve security at lower cost. Even better, this effort would push the network equipment future to sectors where the United States is strongest—in software and semiconductors.

I offered this idea again when I testified a few weeks ago before the Senate Committee on Homeland Security and Government Affairs. It garnered support from witnesses from the Department of Homeland Security, Department of Commerce, and the Department of State. That doesn't always happen in Washington—so we should take advantage of it. Here's what we should do next. The FCC should explore policies to support open RAN and develop testbeds that bring together stakeholders to help

promote more open and interoperable standards. We can even build this effort into our ongoing work to authorize city-wide 5G testbeds in New York and Salt Lake City.

Second, we need to transform the Internet of Things into the Internet of Secure Things. With 5G we are moving to a world with billions of connected devices all around us. But as these connected devices multiply, so do our security vulnerabilities. We need to adjust our policies now because the equipment that connects to our networks is just as consequential for security as the equipment that goes into our networks. And while we may be able to rip and replace the insecure equipment in networks, it would be impractical to think we can do the same for billions of consumer and industrial devices in the Internet of Things.

Here is what we can do. Every device that emits radio frequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products. To do this, we could build on the National Institute of Standards and Technology draft set of security recommendations for devices in the Internet of Things. It covers everything from device identification to device configuration to data protection to access to interfaces to critical software updates. In other words, it's a great place to start—and with billions of new devices coming our way we should get going now.

Third and finally, we need smarter spectrum policy. To date, the FCC has focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. This is a mistake. The rest of the world does not have this singular early focus on high-band, millimeter airwaves, and with good reason. These airwaves have substantial capacity but their signals do not travel far and are easily blocked by walls. As a result, commercializing them is costly—especially in rural areas. The sheer volume of antenna facilities required to make this service viable will limit deployment to the most populated urban areas. This means this agency's early 5G efforts will only deepen the digital divide that already plagues too many communities nationwide.

Moreover, our failure to act early on bringing mid-band spectrum to market has security consequences, too. In many mid-band airwaves worldwide there is only one Chinese vendor offering equipment. That means countries building their 5G networks using this spectrum do not have a competitive choice for secure equipment.

In the United States we have unique skill and scale. That means when deployment takes place here, vendors follow. So it's time for us to make it a priority to make mid-band spectrum available, too. There is no reason why our next auction should be a millimeter wave auction. Instead, we should be clearing the way for the 3.5 GHz band first and following with a C-band auction thereafter. If we can do that, our carriers will build there and more vendors will compete to offer service. And when we expand the market for secure equipment at home, it also grows abroad. That's exactly what we need if we want to encourage diversity in open RAN architectures, too. But best of all, it will mean we can extend the promise of secure 5G wireless service to everyone, everywhere in the country.

Because in the end, that's truly the goal. We want urban America, rural America, and everything in between to know the opportunities of next generation wireless service. But as today's decision and rulemaking make clear—it is not enough just to have access because that access also has to be secure. So if we have vulnerabilities in our networks we need to fix them. If they are in rural areas adjacent to sensitive military installations in Montana or anywhere else across the country we need to replace them. But above all we need to get started. Because this effort represents just that, it has my support.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

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

Network security is national security. As we move into a 5G world where billions of IoT devices will operate our critical infrastructure, health care system, financial sector and transportation systems via mobile wireless transmissions, secure networks are not only necessary to preserve the confidentiality and integrity of our communications, but also to protect our public safety. Today, we take an important step towards protecting these networks by prohibiting the use of universal service funds for the purchase of equipment from the Chinese telecommunications companies Huawei and ZTE. While many talk of security issues surrounding "back doors," I have said many times that the untrustworthy equipment from these companies could readily serve as a "front door" for Chinese intelligence gathering, at the expense of our privacy and national security. I fully support the effort to ban future purchases of such equipment using USF funds.

While that is necessary, it is not sufficient in addressing this issue of national security. Back in May, I published an op-ed first raising my concerns that we cannot afford to think of this issue asymmetrically, focusing strictly on prohibiting untrustworthy equipment from entering our networks, and failing to account for the reality that we already have the same equipment in our infrastructure. Lots of it. I have consistently said that the problem is real, it is here already, and our failure to address existing untrustworthy equipment leaves American citizens vulnerable to data siphoning and foreign interference. That's why I'm glad that we're issuing a Further Notice of Proposed Rulemaking seeking comment on the problem of such equipment and how to address it. As I said back in May, we need to find this untrustworthy equipment, fix the problem, and fund the remedial effort – Find It, Fix It, Fund It.

As today's item discusses, although the data collection we authorize today should provide much more information, our record in this proceeding to date suggests that much of the Huawei and ZTE equipment in our networks is held by certain rural wireless carriers. Since I first spoke on this issue, I've traveled the country and personally met with nearly two dozen of these carriers and their representatives. I held a workshop this summer at the Commission where I heard from rural carriers, equipment manufacturers, national security experts, academics, and various other stakeholders. A few weeks ago, I met with the Department of Homeland Security and the Chamber of Commerce in Denver to discuss these issues with rural carriers. And just yesterday, I published a white paper summarizing the facts, feedback and recommendations that came from those meetings.

Here's what I've learned. These carriers are made up of hard-working men and women that serve hard-to-reach communities that the major carriers can't or won't serve, operating with small teams and tight budgets. And they're worried. They're concerned that they'll be punished for using Chinese equipment in their networks that they bought lawfully and in good faith, in many cases before the full strength of our concerns about network vulnerabilities linked to Chinese telecom manufacturing surfaced. They now understand the significant security risks associated with their Chinese network equipment and software updates. They understand how manufacturers are obligated under Chinese law to cooperate with the government's demands for network access. They understand how their vulnerable equipment could be used for surveillance, disruption of critical services, or cyber-attacks. And they want to fix it. But they need our help, and this FNPRM is the first step on the road to doing so.

But such assistance shouldn't come without considering how we got into this situation and how to avoid duplicating it in the future. Based on information available today, the item indicates that replacing untrustworthy equipment in our networks could cost as much as $2 billion, and the actual figure could be even more. We can't afford to do this again. That's why I proposed the addition of questions seeking comment about what factors led to the dependence of certain carriers on untrustworthy equipment and what measures the Commission could and should take to ensure that all telecommunications carriers obtain and rely on equipment only from trusted vendors. I'm particularly interested in hearing about

American-made alternatives – both hardware and software-based – to untrustworthy or insecure telecom equipment.

As our world becomes even more interconnected, the FCC has a critical role to play in protecting that security. The Commission must be proactive, not reactive, in our national security measures in order to avoid problems like untrustworthy network equipment in the future. And though we've done much, much remains to be done. Here and going forward are a few leading issues on which you will be hearing from me.

First, we need to create an FCC National Security Task Force. The Commission currently reviews national security issues on a distributed basis among the various bureaus. For example, the International Bureau refers applications for Section 214 licenses involving foreign ownership to "Team Telecom" for national security review. The Public Safety and Homeland Security Bureau participates in the National Security Council's NSPM-4 process. And the Wireline Competition and Wireless Telecommunications Bureaus consider national security in license transfers and number portability matters. It remains to be seen which bureau will administer the tremendous task that we vote on here today in setting policy to handle untrustworthy foreign equipment.

This distributed structure makes internal coordination challenging and risks inconsistent treatment of national security issues between different bureaus. These issues are not going to diminish. Quite the opposite, in fact, as I expect that the Commission will continue to see an increase in the number and complexity of issues that will touch on national security. Security issues surrounding Team Telecom, CFIUS, 214 licensing, numbering and so forth are becoming more common. We must be more intentional than ever to ensure that the whole of the FCC is more coordinated, more deliberative, and more collaborative. The FCC should issue a Public Notice creating a National Security Task Force, like other task forces established by the FCC in the past. I look forward to discussing this idea with my colleagues.

Second, as I recently wrote in the San Jose Mercury News, we must seize this opportunity to encourage the growth of American technology for next generation networks. We cannot entrust the technological solutions to the challenges of 5G to geopolitical rivals. Rather, we must support American innovation to meet these challenges. American ingenuity has historically dominated the research, development and deployment of telecommunications technology. This must continue for 5G, and American companies are already developing alternatives to traditional telecom equipment infrastructure through software-enabled 5G and virtualized radio access networks for cloud-based 5G. 5G infrastructure development must represent the next frontier of American technological leadership.

American 5G equipment will be safer because we can be confident about it observing best practices and protecting our intellectual property and privacy from foreign actors. Most importantly, American companies do not answer to the directives of adversary states with no clear rule of law. Moreover, while artificially low prices may have provided a temporary advantage to Huawei and ZTE, I believe that the telecom industry has come to realize that the cost and inconvenience of fixing and replacing untrustworthy equipment far outweighs any short-term savings. I believe America can rise to the challenge and ultimately come out of this situation more advanced, more secure and more prosperous.

Third, our network security depends on the equipment that carries our communications traffic, and critically in some instances also on traffic that leaves our domestic networks. Like many countries around the world, the United States relies on submarine cables to carry its traffic across the oceans. Pending before the Commission now is an undersea cable application from US companies that have partnered with Dr. Peng Telecom & Media Company, one of the largest telecommunications conglomerates in China, for a cable running between Los Angeles and Hong Kong. The project is designed to carry a large portion of the communications between the U.S. and Asia, and a recent Wall Street Journal report indicated that the Justice Department has expressed concerns that the communications could be stolen, blocked, or modified on the Hong Kong end. I share these concerns as an initial matter and want to learn more about what measures can be done, if any, to prevent the Chinese government from eavesdropping, blocking or tampering with these communications.

Finally, the nation's first primaries will take place in a few months. With that in mind, I've been focused on the security of our election system. The threat is real – our intelligence agencies have confirmed that foreign actors sought to tamper with our election systems in 2016 and predict that they will try again in 2020. And while much of the media attention has centered on the use of social media to confuse and polarize us, our networks are also under attack. According to our intelligence agencies, Russian-affiliated cyber actors targeted all 50 state election systems during the 2016 voting cycle, including attacks on voting-related websites and voter registration databases. Although they weren't able to change individual votes or vote totals, we should expect another round of attempts in 2020.

That's one reason why our network security is so important. While completely disconnected voting machines are the most secure, research shows that some states still use the same networks to transmit their voting results that we use for our mobile phones. Indeed, the Federal Election Commission estimates that more than 1,000 of these machines remain in use in states like Wisconsin and Florida.

Once a device is connected to a wireless network, it's subject to the same threats as other wireless communications. Voting results can be blocked or altered by criminals or adversary states using IMSI catchers or by hacking untrustworthy or insecure routers. Because of these risks, I've reached out to the major wireless carriers to discuss how they're protecting their network security and working with election officials. The FCC has a statutory obligation to protect the national defense – the security of our elections clearly qualifies in my mind.

Moving forward, the Commission's policies must reflect the new telecom landscape. The recent influx of new, unfamiliar actors into the telecom space has rendered the old system of operations, built upon trust and familiarity, quaint. I will do everything in my power to keep Americans secure now and in the future. Thank you to my colleagues for their support of my edits to this item and thank you to the Wireline Competition Bureau and the other Commission staff who worked on this item for your excellent work.