UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and
Information Administration
Washington, D.C. 20230

June 9, 2020

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: 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

Dear Chairman Pai:

The National Telecommunications and Information Administration (NTIA), as the President's principal adviser on telecommunications and information policy, and on behalf of the Executive Branch, offers the following views on the Federal Communications Commission's (Commission) "remove and replace" proposal in the Further Notice of Proposed Rulemaking (FNPRM) in the above-captioned proceeding.[1] The Executive Branch applauds the Commission's decision to protect the information and communications technology (ICT) supply chain by prohibiting the use of Universal Service Funds (USF) to acquire equipment or services produced or provided by a covered company posing a national security threat to the integrity of U.S. communications networks. The Executive Branch also agrees that, when properly implemented, rules requiring carriers to remove and replace embedded equipment and services acquired with USF support and produced or provided by covered companies from their networks will provide critical protection to the nation's communications infrastructure and supply chain.

The Executive Branch also fully supports the Commission's initial designation of two Chinese companies – Huawei Technologies and ZTE Corporation – as covered companies.[2] As discussed below, the Executive Branch agrees that the companies' ties to the government of the People's Republic of China (PRC), "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

[1] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation, *Report and Order, Further Notice of Proposed Rulemaking, and Order*, 34 FCC Rcd 11423 (2019) (*FNPRM*). For convenience, unless otherwise indicated, all subsequent citations to "Comments" shall refer to pleadings submitted on February 3, 2020, in WC Dkt. No. 18-89. On April 13, the Commission requested comment on how the proposals in the *FNPRM* may be affected by enactment of the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (to be codified at 47 U.S.C. §§ 1601-1609) (*Secure Networks Act*). *See* FCC, *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission's Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, WC Dkt. No. 18-89, DA 20-406 (rel. Apr. 13, 2020), *available at* https://ecfsapi.fcc.gov/file/04130368802732/DA-20-406A1.pdf.

[2] *See FNPRM*, 34 FCC Rcd at 11439-48, ¶¶ 43-63.

communications networks and the communications supply chain."[3] We urge the Commission to promptly take all actions needed to make those designations final.

Coordination Between the Commission and the Executive Branch

As the Commission moves forward in this proceeding, the Executive Branch urges it to continue to work closely with Executive Branch entities with expertise and responsibilities concerning telecommunications security, including supply chain security. Comments filed in the FNPRM echo the importance of this coordination.[4] As the Commission points out, its actions in this proceeding are part of a larger government-wide effort to prevent foreign adversaries from maliciously creating and exploiting vulnerabilities in the U.S. ICT supply chain.[5] Notably:

- Section 889 of the 2019 National Defense Authorization Act (NDAA) prohibits, *inter alia*, federal agencies from acquiring certain telecommunications equipment or services from specified Chinese suppliers, including Huawei and ZTE, or from contracting with entities that use such equipment or services.[6] The Department of Defense, the General Services Administration, and the National Aeronautics and Space Administration are currently leading the rulemaking effort to implement these prohibitions.[7]

- The SECURE Technology Act, enacted in 2018, established the Federal Acquisition Security Council (FASC), an interagency body that can recommend to the Department of Defense, the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence that certain telecommunications equipment be excluded from

---

[3] *Id*. at 11442, ¶ 48. *See also* Daniel R. Coats, Dir. of Nat'l Intelligence, *Stmt. for the Record: Worldwide Threat Assessment of the US Intelligence Cmty*., at 5, 13-14 (Jan. 29, 2019), *available at* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (discussing the threat to U.S. information and communications technology and services firms from the PRC government).

[4] *See*, *e.g*., Comments of NCTA – The Internet & Television Ass'n in WC Dkt. No. 18-89, at 3-6 (filed Feb. 3, 2020) (NCTA Comments), *available at* https://ecfsapi.fcc.gov/file/10204139929449/NCTA%20Supply%20Chain%20FNPRM%20Comments%202%203%2020%20FINAL.pdf; Comments of the Telecommunications Industry Association in WC Dkt. No. 18-89, at 5-11, (filed Feb. 3, 2020) (TIA Comments), *available at* https://ecfsapi.fcc.gov/file/10203229746606/TIA%20Final%20USF%20Comments.pdf; and Comments of USTelecom – The Broadband Association in WC Dkt. No. 18-89, at 7-9 (filed Feb. 3, 2020) (US Telecom Comments), *available at* https://ecfsapi.fcc.gov/file/102042351015335/2-3-20%20USTelecom%20FCC%20Supply%20Chain%20NPRM%20Comments%20Final.pdf.

[5] *See FNPRM*, 34 FCC Rcd at 11427-29, ¶¶ 12-17.

[6] *See* John S. McCain National Defense Authorization Act for Fiscal Year of 2019, Pub. L. No. 115-232, § 889(a), 132 Stat. 1636, 1917 (2018).

[7] *See, e.g*., Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, 84 Fed. Reg. 68,314 (Dec. 13, 2019); Federal Acquisition Regulation: Reporting of Nonconforming Items to the Government-Industry Data Exchange Program, 84 Fed. Reg. 64,680 (Nov. 22, 2019); Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, 84 Fed. Reg. 40,216 (Aug. 13, 2019).

federal procurements on national security grounds. The Act authorizes those agencies to prohibit government procurement of such equipment.[8]

- In May 2019, the President issued an Executive Order directing the Secretary of Commerce, in consultation with heads of other agencies including the Chairman of the Commission, to prohibit or mitigate certain ICT-related transactions that involve a foreign adversary and pose an undue or unacceptable risk to U.S. national security or the security and safety of U.S. persons.[9] The Commerce Department is preparing regulations to implement that directive.[10]

Additionally, the Executive Branch is engaged in several other related security and supply chain efforts that should support and inform the Commission's effort.[11] As the Commission is aware, DHS's Cybersecurity and Infrastructure Security Agency, for example, leads the Executive Branch's cybersecurity preparedness efforts across all levels of government and currently hosts an ICT Supply Chain Task Force with government and private sector participants under the auspices of its Critical Infrastructure Partnership Advisory Council authority.[12] The Department of Defense, via its Cybersecurity Maturity Model Certification initiative, is currently reviewing and combining industry cybersecurity standards and best practices into one unified framework.[13] The Commerce Department's National Institute of Standards and Technology is devising standards to guide the nation's supply chain security and risk management practices.[14]

---

[8] SECURE Technologies Act, Pub. L. 115-390, Tit. II, § 202, 132 Stat. 5173 (2018) (to be codified at 41 U.S.C. § 1323(c)).
[9] Exec. Order No. 13873, 84 Fed. Reg. 22,689 (2019).
[10] *See* Securing the Information and Communications Technology and Services Supply Chain, *Proposed Rule and Request for Comments*, 84 FR 65316 (Nov. 27, 2019).
[11] For example, the President recently issued Executive Order 13913, "Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector," which formalized the process by which the Executive Branch advises the Commission on national security and law enforcement concerns related to certain applications to the Commission or licenses issued by the Commission. *See* Exec. Order No. 13913, 85 Fed. Reg.19643 (2020).
[12] *See* U.S. Dep't of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report* (Sept. 2019), *available at* https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf; U.S. Dep't of Homeland Security, *Charter of the Critical Infrastructure Partnership Advisory Council (*Nov. 2018), *available at* https://www.cisa.gov/sites/default/files/publications/cipac-charter-november-30-2018-508.pdf.
[13] U.S. Dep't of Defense, *Cybersecurity Maturity Model Certification (CMMC): CMMC Model v1.0* (Jan. 31, 2020), *available at* https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf.
[14] *See*, *e.g.*, U.S. Dep't of Commerce, National Institute of Standards and Technology, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, Draft NISTIR 8286 (Mar. 2020), *available at* https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286-draft.pdf.

NTIA is promoting policy and coordinating a stakeholder-driven process toward the development of a "software bill of materials," which will improve the marketplace's ability to monitor, detect, and mitigate software supply chain risks.[15] NTIA also co-chairs a working group formed in conjunction with the non-profit Alliance for Telecommunications Industry Solutions (ATIS), to create 5G-focused supply chain standards and guidelines. Additionally, through the recent passage of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), Congress directed NTIA to establish a program to share information regarding supply chain security risks with trusted providers of communications equipment or services.[16]

The Executive Branch agrees with commenters that continued close collaboration between the Commission and other federal actors is essential to ensure that, in crafting the Commission's supply chain regulations, "no relevant expertise, proceeding, or policy interest within the U.S. government is overlooked."[17] Of critical importance, such collaboration will limit the potential for duplication of effort or inconsistent or conflicting results that would create ambiguity in the marketplace, increase the costs of compliance and administration for market players, or potentially allow vulnerabilities within the U.S. supply chain to persist without mitigation. Further, collaboration should not be limited to the implementation of remove and replace. It should also inform the process by which the Commission designates covered companies,[18] or reexamines the equipment and services that may not be procured by USF recipients.[19]

Designating Huawei and ZTE as Covered Companies

As previously noted, the Executive Branch supports the Commission's initial designation of two companies headquartered in the PRC – Huawei Technologies and ZTE Corporation – as covered companies. Although the extent of direct PRC government ownership of Huawei and ZTE is uncertain,[20] those companies, like other Chinese ICT vendors, are beholden legally and

---

[15] *See* U.S. Dep't of Commerce, NTIA, *NTIA: Software Component Transparency* (Apr. 14, 2020), *available at* https://www.ntia.doc.gov/SoftwareTransparency.

[16] *See* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 8(a), 134 Stat. 158, 168 (2020) (to be codified at 47 U.S.C. §§ 1601-1609) (*Secure Networks Act*).

[17] TIA Comments at 5.

[18] *See FNPRM*, 34 FCC Rcd at 11438-39, 11449, ¶¶ 39-42, 64-65.

[19] Indeed, the Commission may need to revisit its procurement ban on "any and all equipment or services produced or provided" by a covered company. *Id*. at 11449, ¶ 66. The recently-enacted Secure Networks Act bars the use of monies from specified USF programs to acquire or maintain equipment or services on a Commission-established list. Secure Networks Act, Pub. L. No. 116-124, § 3(a). The Act further directs that the Commission may include particular equipment or services on that list "if and only if" it has defined characteristics or capabilities, or it poses an unacceptable risk to national security or public safety. *Id*. § (b)(1), (2), 134 Stat. at 158. In making that latter determination, the Commission must rely "solely" on the NDAA or "specific determination[s]" by Executive Branch agencies. *See id*. § 2(c), 134 Stat. at 158-59. The Commission's rationale for applying its procurement ban to all equipment and services does not cite decisions by such agencies. *See FNPRM*, 34 FCC Rcd at 11449-53, ¶¶ 66-76. It also indicates that the decision was made, at least in part, to "provide regulatory certainty and . . . be easier for providers to implement and for the Commission to enforce," as well as to "level the competitive playing field." *Id*. at 11450, ¶ 69.

[20] The Chinese government may have a minority stake in ZTE. *See FNPRM,* 34 FCC Rcd at 11447*,* ¶ 60.

extralegally[21] to the PRC government and the Chinese Communist Party (CCP). Starting in 2014, the CCP has enacted an interrelated package of national security, cyberspace, and law enforcement legislation, including the Counterespionage Law (2014), the National/State Security Law (2015), the Counterterrorism Law (2015), the Foreign Non-Governmental Organization Law (2016), the Cybersecurity Law (2017), the National Intelligence Law (2017), and the Cryptography Law (2019).

The National Intelligence Law (NIL) and the Cybersecurity Law (CL), in particular, impose affirmative legal responsibilities on PRC and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for the government's intelligence gathering activities. For example, Article 7 of the NIL states, "[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets that they are aware of."[22] Article 14 declares that PRC intelligence organs "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation." Article 16 expressly allows Chinese intelligence organs to enter companies' restricted areas and collect files at will. Article 17 goes even further, providing that intelligence services may "have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings; and when necessary, they may set up relevant work sites, equipment, and facilities." The law provides no ability, check, or balance for companies or individuals to refuse these requests. The law leaves most terms undefined, allowing for arbitrary interpretations that suit the interests of the CCP.

Article 28 of the CL, in turn, compels all network provider operators to "provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[23] Taken together, these laws empower the PRC government to make extensive, affirmative demands on Chinese companies and their officers and employees to advance the CCP's intelligence gathering interests.

---

[21] Regardless of the explicit legal obligations of Chinese companies, all aspects of society are subject to the arbitrary authority of the CCP. A 2018 amendment to the PRC constitution made clear that the "leadership of the Communist Party of China is the defining feature of socialism with Chinese characteristics." *Amendment to the Constitution of the People's Republic of China* (Mar. 2018), *available at* http://www.fdi.gov.cn/1800000121_39_4866_0_7.html. Moreover, the PRC's power to compel, from individuals to the largest corporations, exists outside any legal framework and, thus, is not limited by any law.

[22] This and subsequent quotations from the NIL are taken from China Law Translate, *National Intelligence Law of the P.R.C.* (June 2017), *available at* https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.

[23] *See* Rogier Creemers, Paul Triolo, and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China* (enacted Nov. 6, 2016, effective June 1, 2017), *available at* https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. *See also* William Evanina, *Keynote Remarks*, International Legal Technology Association (ILTA) LegalSEC Summit 2019 (June 4, 2019), *available at* https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.

The Chinese judiciary also lacks the independence and power to check the demands of the government or the CCP. As Chinese leader Xi Jinping stated in 2019, "[w]e must never follow the path of Western 'constitutionalism,' 'separation of powers,' or 'judicial independence.'"[24] Under Chinese law, one of the conditions for becoming a judge is "[s]upporting the Constitution of the People's Republic of China and the leadership of the Communist Party of China and the socialist system."[25] The CCP, through people's committees at various levels of PRC government (e.g., national, provincial, townships), also appoints, dismisses, transfers, and promotes judges.[26] The CCP Constitution provides that courts fall under the jurisdiction of local governments, which also appropriate courts' budgets.[27] Consequently, Chinese courts cannot be expected to render judgments contrary to the interests of the government or the Party.

In addition to these legal controls, the CCP has the ability to influence decision-making at all levels within Chinese companies, both state-owned and private. In accordance with PRC law, both Huawei and ZTE maintain internal Communist Party Committees.[28] Since 2017, the CCP Constitution has required Party cells in state-owned enterprises (SOEs) to "ensure the implementation of Party policies and principles," "decide on major issues of their enterprise," and "support the board of shareholders, board of directors, board of supervisors, and manager (or factory director) in exercising their functions and powers."[29] Although the committees' activities may be less pervasive in private companies, Huawei has acknowledged that PRC law authorizes

---

[24] *See* Charlotte Gao, *Xi: China Must Never Adopt Constitutionalism, Separation of Powers, or Judicial Independence*, The Diplomat (Feb. 19, 2019), *available at* https://thediplomat.com/2019/02/xi-china-must-never-adopt-constitutionalism-separation-of-powers-or-judicial-independence/. Xi's article is available in Chinese at Xi Jinping, *Strengthening the Party's Leadership over the Rule of Law*, Qiushi Journal (Apr. 2019), *available at* http://www.qstheory.cn/dukan/qs/2019-02/15/c_1124114454.htm. The 2017 CCP Constitution states that the "party exercises overall leadership over all areas of endeavor in every part of the country." *Constitution of the Communist Party of China* at 10 (Oct. 24, 2017), *available at* http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf (*CCP Constitution*). A 2019 intraparty regulation restates the Party's "absolute leadership over political-legal work." China Law Translate, *Regulation on the Communist Party of China's Political-Legal Work*, Art. 7 (Jan. 18, 2019), *available at* https://www.chinalawtranslate.com/en/regulation-on-the-communist-party-of-chinas-political-legal-work/.

[25] *See* China Translate, *Judge Law of the People's Republic of China*, Art. 12, ¶ 2 (2019), *available at* https://www.chinalawtranslate.com/judges-law-of-the-prc-2019/.

[26] *Id*., Art. 18.

[27] *Amendment to the Constitution of the People's Republic of China* (Mar. 2018) (amending Art. 37, ¶ 3, Art. 3 of the PRC Constitution), *available at* http://www.fdi.gov.cn/1800000121_39_4866_0_7.html.

[28] *See FNPRM,* 34 FCC Rcd at 11447, ¶ 60.

[29] *CCP Constitution*, Art. 33.

the committees within private entities to "provide[] guidance to and oversee[] the enterprise in strictly observing the laws and regulations of the state."[30]

Further, the CCP Constitution also requires private companies to carry out Party policies. The PRC requires joint ventures to give CCP cells legal standing within their corporate governance structure whenever an SOE is a party in the venture.[31] PRC securities regulations even require companies to allow CCP cells to carry out Party activities inside the company as a condition of listing shares,[32] which in practice has led essentially all SOEs and many private companies to amend their charters to give the CPP a formal role in corporate governance.[33]

The fact that maintaining a good relationship with the CCP is a prerequisite for business success has led companies like Huawei to be active participants in achieving the goals of the State. In Xinjiang, China, Huawei has supported the surveillance and detention of over a million Uighurs, depriving them of their freedom and their human rights.[34] The company closely cooperates with the Xinjiang Public Security Bureau, including through the development of data center infrastructure and agreement to establish an "intelligent security industry" innovation lab.[35] Huawei has also signed a strategic agreement with the State-owned Xinjiang Broadcasting and

---

[30] Comments of Huawei Technologies Co., LTD., and Huawei Technologies USA, Inc. in PS Dkt. No. 19-351, at 136 (filed Feb. 3, 2020), *available at* https://ecfsapi.fcc.gov/file/102030067606114/Huawei%20Designation%20Comments%20Docket%20No.%2019-351.pdf.

[31] *See* Simon Denyer, *Command and control: China's Communist Party extends reach into foreign companies*, The Washington Post (Jan. 28, 2018), *available* at https://www.washingtonpost.com/world/asia_pacific/command-and-control-chinas-communist-party-extends-reach-into-foreign-companies/2018/01/28/cd49ffa6-fc57-11e7-9b5d-bbf0da31214d_story.html.

[32] *See Code of Corporate Governance for Listed Companies*, Art. 5 (2018), *available at* http://www.csrc.gov.cn/pub/csrc_en/laws/rfdm/DepartmentRules/201904/P020190415336431477120.pdf

[33] *See* Lauren Yu-Hsin Lin and Curtis Milhaupt, *Party Building or Noisy Signaling? The Contours of Political Conformity in Chinese Corporate Governance*, European Corporate Governance Inst. – Law Working Paper No. 493/2020; Stanford Law and Economics Olin Working Paper No. 545, City University of Hong Kong Centre for Chinese and Comparative Law Research Paper Series No. 2020/005, at 2-3 (Revised Feb. 2020), *available at* https://poseidon01.ssrn.com/delivery.php?ID=484029088111001004079102094000127072016089038039060053007117009027101107086071088109010114056102019017037122124031072080005112048032033082076104114109116090108003108007092010066122084090116112076087113003080126120089118019025076012082018093073071113085&EXT=pdf (finding that a significant number of private enterprises, particularly politically connected ones, have amended their charters to add party-building provisions).

[34] Fergus Ryan, Danielle Cave and Vicky Xu, *Mapping more of China's technology giants*, at 3, 5, 20-21, Australian Strategic Pol. Instit. Rep. No. 24 (Nov. 2019), *available at* https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-12/Mapping%20more%20of%20Chinas%20tech%20giants.pdf?wpDVHlKgXJHzeK8rZ.kmy0Ei63RxXMO.

[35] *Id*. at 20-21.

Television Network Co. Ltd. aimed at "maintaining social stability and creating positive public opinion."[36]

As long as Huawei and ZTE are subject to the legal and extralegal influence and control of the Chinese government and the CCP, there are doubts that the companies can be trusted to comply fully with U.S. law, as Attorney General Barr recently informed the Commission.[37] Huawei has allegedly offered bonuses to its employees based on the value of information they stole from other globally-situated companies.[38] Even where the companies' personnel in the United States may be willing to follow U.S. law, they can be circumvented. As Attorney General Barr noted, a federal grand jury has alleged that Huawei sent employees from China to steal intellectual property from T-Mobile when employees in the U.S. were unwilling or unable to do as the company's Chinese executives directed.[39] The PRC government can also recruit employees of Chinese companies doing business in the U.S. to engage in illegal activity here. Last year, for example, a former airline ticket counter agent pleaded guilty to acting as an agent of the Chinese government by working at the direction and control of military officers assigned to China's Mission to the United Nations. She encouraged her coworkers to assist the military officers, telling them that, because the Air Carrier was a Chinese company, their primary loyalty should be to China.[40]

Further, both ZTE and Huawei pose a risk to U.S. national security based on their activities in violation of U.S. law. ZTE has pleaded guilty to engaging in a multi-year conspiracy to supply, build, and operate telecommunications networks using U.S.-origin equipment in violation of the U.S. trade embargo on Iran, and committing hundreds of U.S. sanctions violations involving the shipment of telecommunications equipment. Moreover, ZTE also made false statements and obstructed justice by creating an elaborate scheme to prevent disclosures to and mislead the U.S. Government. Even after the guilty plea, ZTE continued to make false statements to U.S. authorities and pursuant to a June 2019 settlement agreement with the Bureau of Industry and Security (BIS) agreed to pay $1 billion in penalties. Huawei remains on the BIS Entity List for its activities that are contrary to U.S. national security and foreign policy interests, including alleged violations of the International Emergency Economic Powers Act (IEEPA), conspiracy to violate IEEPA by providing prohibited financial services to Iran, and obstruction of justice in connection with the investigation of those alleged violations of U.S. sanctions.

Funding for Remove and Replace

Through passage of the Secure Networks Act, Congress recently facilitated the implementation of a remove and replace program by directing the Commission to establish a reimbursement program.[41] The Secure Networks Act also requires the Commission to notify Congress if costs

---

[36] *Id*. at 21.
[37] *See* Letter from Attorney General William Barr to Chairman Ajit Pai, at 2-3 (Nov. 13, 2019), *available at* https://ecfsapi.fcc.gov/file/111501201939/18-89A.pdf.
[38] *Id*. at 1.
[39] *Id*.
[40] U.S. Dep't of Justice, *Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government* (Apr. 17, 2019), *available at* https://www.justice.gov/opa/pr/former-manager-international-airline-pleads-guilty-acting-agent-chinese-government.
[41] *See Secure Networks Act*, § 4(a), 134 Stat. at 160.

for the program will exceed $1 billion.[42] The Commission is also currently collecting data from potentially affected carriers about the equipment and services they have obtained from covered companies, "the costs associated with purchasing and/or installing such equipment and services; and the costs associated with removing and replacing such equipment and services."[43] According to recent Commission estimates, the costs of a remove and replace program could be between $1 billion and $2 billion.[44] Some commenters contend that the Commission has sufficient authority to fund all or some portion of a reimbursement program through its existing USF program. The Secure Networks Act's mandate that the Commission keep the remove and replace program separate from its other USF programs, however, may constrain the agency's flexibility in this area.[45] Moreover, the President has committed to "use all possible policy tools to accelerate the deployment and adoption of affordable, secure, reliable, modern high-speed broadband connectivity," and diverting limited USF funds at this time could undermine this goal at a critical time, notably during the COVID-19 pandemic.[46] Consequently, the Commission should promptly seek funding from Congress to support costs for the reimbursement program.[47]

Elements of a Remove and Replace Program

The Commission must ensure that implementation of a remove and replace program for USF recipients is consistent with the foundational goals of universal service – availability of quality service at just, reasonable, and affordable rates at a comparable level of service to all Americans.[48] Although the Commission reasonably concludes that "providing a secure service is part of providing a quality service,"[49] available features and functions, performance

---

[42] *See id.*, (d)(5)(B), 134 Stat. at 162-63.
[43] *See* FCC, *Wireline Competition Bureau and Office of Economics and Analytics Open Reporting Portal for Supply Chain Security Information Collection*, WC Dkt. No. 18-89, DA 20-166 (rel. Feb. 26, 2020), *available at* https://docs.fcc.gov/public/attachments/DA-20-166A1.pdf.
[44] *See FNPRM*, 34 FCC Rcd at 11481, ¶ 161 (program costs may reach $2 billion if remove and replace completed within two years, $1.41 billion if the transition period is seven years). *See also* Letter from the Honorable Ajit Pai, Chairman, Federal Communications Commission, to Senators John Kennedy and Chris Coons, Mar. 14, 2020.
[45] *See, e.g.,* NTCA Comments at 5; comments of the Rural Wireless Broadband Coalition in WC Dkt. No. 18-89 at 3 (filed Feb. 3, 2020), *available at* https://ecfsapi.fcc.gov/file/1020334786638/2020%200203%20RWB%20Coalition%20Comments%20-%20Supply%20Chain%20Further%20NPRM%20-%20FINAL%20As%20Filed.pdf. *See also Secure Networks Act*, § 4(j) (remove and replace program "shall be separate from any Federal universal service program established under section 254").
[46] Exec. Order No. 13821, 83 Fed. Reg. 1507 (2018). *See* also U.S. Dep't of Commerce, National Telecommunications and Information Administration, *American Broadband Initiative: Milestones Report – February 2019, available at* https://www.ntia.doc.gov/files/ntia/publications/american_broadband_initiative_milestones_report.pdf.
[47] *See Secure Networks Act* § 4(d)(5)(B), 134 Stat. at 162-63 (directing Commission to notify the Senate and House Commerce and Appropriations Committees if it determines that $1 billion will not be sufficient to fully fund all approved applications for reimbursements under the program).
[48] *See* 47 U.S.C. § 254(b)(1), (3). As a rule, the equipment and services subject to a remove and replace obligation should parallel the equipment and services covered by the prospective procurement ban.
[49] *See FNPRM*, 34 FCC Rcd at 11434, ¶ 29.

characteristics, and reliability are also paramount to service quality for users. The goals of the Administration's actions and the Congressional legislation are to block untrustworthy equipment from entering our domestic infrastructure and to replace with immediacy any existing untrusted equipment.[50] The Commission, therefore, should immediately identify means to help affected carriers acquire trusted equipment.

As for service comparability, recipients of USF funds are typically subject to both minimum service and geographic deployment requirements.[51] Thus, any remove and replace reimbursement program must, at a minimum, ensure that affected carriers can acquire alternative equipment and services that will enable them to satisfy their minimum service and buildout obligations. That may not be sufficient, however, because as the Commission is aware, minimum service requirements must change over time to preserve comparability between USF-supported services and those available to other parts of the country. Consequently, limiting reimbursement to "like for like" replacements may "lock-in [USF] carriers to equipment that may become rapidly outdated or threaten to exacerbate the digital divide."[52] For that reason, the Commission should give carriers a level of flexibility to use reimbursement monies to purchase equipment that can support, or can readily be upgraded to support, more advanced levels of service. This would also reinforce the President's goal "to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide."[53] The Commission should also look favorably upon the use of reimbursement monies in ways that further Administration priorities in the President's National Strategy to Secure 5G, such as strategies that reinforce 5G vendor diversity and foster market competition.[54]

Similarly, as the Commission recognizes, some USF recipients that acquired equipment and services from covered companies benefited from "favorable subsidies and other benefits bestowed" by the suppliers' home government. Any Commission reimbursement program should make some accommodation for those USF recipients, in a manner also consistent with the significant security benefits of removing such equipment and services.[55]

---

[50] The Commission's Order took effect "immediately upon publication in the Federal Register," which occurred on January 3, 2020. *See id*. at 11482, ¶ 167; 85 Fed. Reg. 230 (2020).
[51] *See* 47 C.F.R. §§ 54.308-54.312.
[52] Nokia Comments at 7.
[53] *National Strategy to Secure 5G of the United States of America* at i (Mar. 2020), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.
[54] *Id.* at 6.
[55] The Commission requests comment on the potential security risks to users from carrier distribution to Lifeline subscribers of free wireless handsets acquired from covered companies. The Commission raises the issue here while also examining the benefits and risks of free handset distribution in a separate proceeding, although there is broad public and industry support for such distribution. *See* Bridging the Digital Divide for Low-Income Consumers, *Fifth Report and Order, Memorandum Opinion and Order and Order on Reconsideration, and Further Notice of Proposed Rulemaking*, 34 FCC Rcd 10886, 10949-52, ¶¶ 151-58 (rel. Nov. 14, 2019). The Commission does not express similar concern about the risks to consumers' communications posed by the distribution of covered companies' handsets by non-Lifeline providers on other terms. If the Commission is concerned about the security risk presented by the continued use of suspect handsets, it has ample authority to alter wireless providers' radio licenses to bar them from permitting the use of such devices on their networks. *See* 47 U.S.C. § 316(a) (giving the Commission broad authority to impose prospective conditions on radio

Thank you for the consideration of these views.

Respectfully submitted,

Douglas Kinkoph

Douglas W. Kinkoph,
Associate Administrator, Office of Telecommunications and Information Applications, Performing the Non-Exclusive Functions and Duties of the Assistant Secretary of Commerce for Communications and Information

cc: The Honorable Michael O'Rielly
The Honorable Brendan Carr
The Honorable Jessica Rosenworcel
The Honorable Geoffrey Starks

licenses at any time in furtherance of the public interest). *See also* Amendment of Parts 1, 2, 22, 24, 27, 90 and 95 of the Commission's Rules to Improve Wireless Coverage Through the Use of Signal Boosters, *Report and Order*, 28 FCC Rcd 1663, 1671-75, ¶¶ 22-30 (2013) (rather than requiring individual licensing of consumer transmitting devices in accordance with section 301 of the Communications Act, authorization is included in the license of the entity providing the underlying service).