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	)	PS Docket No. 19-351
Programs – Huawei Designation	)	
	)	

ORDER

Adopted: June 30, 2020 **Released: June 30, 2020**

By the Chief, Public Safety and Homeland Security Bureau:

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Order, the Public Safety and Homeland Security Bureau (Bureau) takes action to protect America's communications networks and the communications supply chain from the national security threat posed by Huawei Technologies Company (Huawei). In November 2019, the Commission adopted a rule to prohibit the use of universal service support to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.[1] The Commission also initially designated two companies, including Huawei, as covered companies for the purposes of this rule, and

[1] 47 CFR § 54.9(a); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11433, para. 26 (2019) (*Protecting Against National Security Threats Order* or *Order*).

directed the Bureau to determine whether to issue final designations of those companies.[2] Based on the totality of evidence before us, the Bureau hereby issues this final designation of Huawei, as well as its parents, affiliates, and subsidiaries, as a covered company for purposes of this rule.[3] As a result of today's action, funds from the Commission's Universal Service Fund may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by Huawei.

II. BACKGROUND

2. 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 . . . ."[4] The Commission has therefore taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats. In particular, on November 22, 2019, the Commission adopted the *Protecting Against National Security Threats Order* (*Order*), which barred the use of universal service support to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.[5] The Commission adopted this rule based on its conclusion that it is critical to the provision of "quality service"[6] that Universal Service Fund (USF) funds be spent on secure networks and not be spent on equipment and services from companies that threaten national security.[7]

3. In the *Order*, the Commission also adopted a process to identify and designate companies as national security threats for purposes of its rule.[8] Consistent with this process, the Bureau is required to issue a public notice announcing its final designation and make a final designation effective no later than 120 days after release of the initial designation notice, with the ability to extend such deadline for good cause.[9]

4. Following an extensive examination of the record, in the *Order*, the Commission initially designated Huawei and ZTE Corporation (ZTE) as covered companies for purposes of its rule.[10] The Commission initially designated Huawei because it found that Huawei and ZTE posed "a unique threat" to the security and integrity of the nation's communications networks and communications supply chain because of their size, their close ties to the Chinese government, and the security flaws identified in their equipment.[11] The Commission noted that Huawei's ties to the Chinese government and military

[2] *Order*, 34 FCC Rcd at 11439-40, 11449, paras. 43, 64.

[3] 47 CFR § 54.9(a).

[4] 47 U.S.C. § 151.

[5] 47 CFR § 54.9(a); *Order*, 34 FCC Rcd at 11433, para. 26.

[6] 47 U.S.C. § 254(b)(1).

[7] *Order*, 34 FCC Rcd at 11434, para. 29.

[8] 47 CFR § 54.9(b); *Order*, 34 FCC Rcd at 11438-39, 11449, paras. 39-42, 64.

[9] *Order*, 34 FCC Rcd at 11438, 11449, paras. 40, 64. *See also* 47 CFR § 54.9(b)(2). The Bureau released a Public Notice announcing publication of the initial designation in the Federal Register on January 3, 2020. *Public Safety and Homeland Security Bureau Announces Comment Date on the Initial Designation of ZTE Corporation as a Covered Company in the National Security Supply Chain Proceeding*, PS Docket No. 19-352, Public Notice, DA 20-14 (PSHSB Jan. 3, 2020). The Bureau subsequently found good cause to extend the 120-day deadline for determining whether to issue final designations of ZTE and Huawei to June 30, 2020. *Public Safety and Homeland Security Bureau Extends Timeframe Whether to Finalize Designations of Huawei and ZTE Pursuant to 47 CFR § 54.9*, PS Docket Nos. 19-351 and 19-352, Public Notice, DA 20-471 (PSHSB 2020).

[10] *Order*, 34 FCC Rcd at 11439-40, para. 43.

[11] *Order*, 34 FCC Rcd at 11439-41, paras. 43-46.

apparatus, along with Chinese laws obligating it to cooperate with requests by the Chinese government to use or access its system, and the Chinese government's general non-adherence to the law in any event, make it susceptible to Chinese governmental pressure to participate in espionage activities.[12] The Commission also relied on reports highlighting known cybersecurity risks and vulnerabilities in Huawei equipment, which have led other countries to bar the use of such equipment.[13] Furthermore, the Commission was informed by the steps taken by Congress and the Executive Branch to restrict the purchase and use of Huawei equipment, including the Department of Defense's decision to remove Huawei devices from sale at U.S. military bases and from its stores worldwide.[14] In addition, the Commission observed that Huawei's founder, Ren Zhengfei, previously served as a director in the People's Liberation Army of China (PLA), the armed forces of China and its ruling Communist Party, and that former Huawei employees have provided evidence showing that Huawei provides network services to an entity believed to be an elite cyber-warfare unit within the PLA.[15] The Commission further explained that Huawei has been "reported to receive vast subsidies from the Chinese government."[16]

5. After the initial designation of Huawei, the Commission directed the Bureau to implement the next steps in the designation process.[17] Following the publication of the *Order* in the Federal Register, interested parties were provided 30 days to file comments responding to the initial designation.[18] Huawei filed comments raising numerous factual and legal arguments. More specifically, Huawei challenged the initial designation by arguing that the Commission relied on unsupported conclusions about Chinese law that ignored Huawei's multiple expert submissions, that the Commission's decision to "selectively" target Huawei was arbitrary and capricious, and that the designation was "infected" by unconstitutional congressional pressure and unconstitutional prejudgment against Huawei.[19] Huawei further contended the Commission should not issue a final designation of Huawei as a covered company under the Commission's rule because the initial designation was invalid and could not be relied upon by the Bureau, and because additional evidence showed that designation of Huawei was improper.[20] Finally, Huawei took the position that the Bureau could not enter a final designation without providing Huawei with additional procedural safeguards.[21]

6. Recently, on March 12, 2020, the President signed into law the Secure and Trusted Communications Networks Act of 2019 (the Secure Networks Act).[22] The Secure Networks Act directs the Commission to publish a list of covered equipment or services that pose an unacceptable risk to U.S. national security. Most relevant here, the Secure Networks Act requires the Commission to include on the list telecommunications equipment or services covered in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA), which includes telecommunications equipment produced by Huawei or its subsidiaries and affiliates,[23] so long as the equipment or service is capable of

[12] *See Order*, 34 FCC Rcd at 11442, paras. 48.

[13] *See Order*, 34 FCC Rcd at 11444-47, paras. 53-57.

[14] *See Order*, 34 FCC Rcd at 11442, 11444, paras. 48, 52.

[15] *See Order*, 34 FCC Rcd at 11443, para. 50.

[16] *Order*, 34 FCC Rcd at 11443-44, para. 51.

[17] *Order*, 34 FCC Rcd at 11449, para. 64.

[18] Federal Communications Commission, Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation, 85 Fed. Reg. 230, 236 (Jan. 3, 2020).

[19] *See* Huawei Comments at 36-124.

[20] *See* Huawei Comments at 124-62.

[21] *See* Huawei Comments at 162-76.

[22] *See* Pub. L. 116-124, 133 Stat. 158 (2020) (Secure Networks Act).

routing or redirecting user data traffic or permitting visibility into user data or packets, causing network traffic to be disrupted remotely, or otherwise poses an "unacceptable risk" to U.S. national security or the security and safety of U.S. persons.[24] The Secure Networks Act further prohibits use of federal subsidy funds, such as the Universal Service Fund, to purchase, rent, lease, or otherwise obtain, or to maintain, listed communications equipment or services, and further designates reimbursement funds for eligible service providers to remove and replace such listed equipment or services.[25]

7. On March 13, 2020, the Bureau released a public notice seeking comment on the applicability of the Secure Networks Act to this designation proceeding.[26] Huawei filed comments arguing that the Secure Networks Act is "irrelevant" to the designation proceeding, except that it evidences the Commission's lack of authority to adopt regulations that have the objective of protecting national security.[27] Four other commenters—Parallel Wireless, Rural Wireless Association, USTelecom, and WTA – Advocates for Rural Broadband—argued that we should delay a final designation of Huawei until the Commission implements the requirements of the Secure Networks Act. In addition, some commenters contended that the Secure Networks Act requires us to limit the scope of the designation by extending our prohibition only to that equipment specifically prohibited in the Secure Networks Act.[28]

8. On June 9, 2020, the National Telecommunications and Information Administration (NTIA) submitted a filing in this proceeding explaining that the Executive Branch "fully supports" the initial designations of Huawei and ZTE and providing the Executive Branch's analysis of matters including the legal framework in China, the national security risks posed specifically by Huawei and ZTE, and the national security interests demonstrated by their violations of U.S. law.[29] The Bureau

(Continued from previous page)

[23] *See* Pub. L. 115-232, 132 Stat. 1918, § 889(f)(3)(A) (2019 NDAA) (defining "covered telecommunications equipment or services" as meaning telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities).

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

[25] *See id.* at §§ 3-4. The Secure Networks Act specifically preserves any action taken by the Commission before the implementation of its prohibitions to the extent that such actions are consistent with section 3 of the Secure Networks Act. *See* Secure Networks Act § 3(b).

[26] *See Public Safety and Homeland Security Bureau Seeks Comment on Applicability of Secure and Trusted Communications Networks Act of 2019 to Initial Designation Proceedings of Huawei and ZTE*, Public Notice, PS Docket Nos. 19-351, 19-352, DA 20-267 (PSHSB Mar. 13, 2020).

[27] *See* Huawei Secure Networks Act PN Comments at 3.

[28] *See* USTelecom PN Comments at 3-5; WTA-Advocates for Rural Broadband PN Comments at 2-5.

[29] *See* Letter from Douglas W. Kinkoph, Associate Administrator, Office of Telecommunications and Information Applications, National Telecommunications and Information Administration, to Ajit Pai, Chairman, Federal Communications Commission, PS Docket Nos. 19-351, 19-352; WC Docket No. 18-89 (filed June 9, 2020) (NTIA Letter). We note that the Commission has historically found it appropriate to seek and accord deference to the expressed views of the Executive Branch in identifying and interpreting issues of national security, law enforcement, and foreign policy. *See Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, FCC 97-398, 12 FCC Rcd 23891, 23919, para. 63 (1997); *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, FCC 19-38, 34 FCC Rcd 3361, 3362-63, para. 2 (2019).

provided an opportunity for Huawei and other interested parties to respond by seeking comment on this filing on June 9, 2020.[30] Four parties, including Huawei, filed comments in response to NTIA's filing.[31]

III. DISCUSSION

9. We issue this final designation of Huawei as a covered company for purposes of the Commission's rule prohibiting the use of USF funds to purchase or obtain equipment or services from a company posing a national security threat to the integrity of communications networks or the communications supply chain. Pursuant to the *Protecting Against National Security Threats Order*, when designating an entity as a "covered company," we are to base our determination "on the totality of the evidence surrounding the affected entity and should consider any evidence provided by the affected entity, or any other interested party," in making a final determination.[32] The *Order* further provides that, in formulating initial and final designations, we are to use all available evidence to determine whether an entity poses a national security threat.[33] 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.[34]

10. We conclude, based on the evidence supporting the Commission's initial designation and an assessment of the totality of evidence before us, including filings submitted in the record by Huawei and all other interested parties, that Huawei poses a national security threat to our nation's communications networks and the communications supply chain.[35] Accordingly, USF recipients may not use USF funds to purchase, obtain, maintain, improve, modify, manage, or otherwise support Huawei equipment or services in any way, including upgrades to existing Huawei equipment and services.[36]

A. Huawei Poses a National Security Threat to the Integrity of Our Communications Networks and the Communications Supply Chain

11. In the *Order*, the Commission identified Huawei as posing a particular threat to U.S. national security interests based on its substantial ties to the Chinese government and military apparatus, as well as Chinese laws obligating it to cooperate with any Chinese government request to use or access its systems for intelligence and surveillance.[37] The *Order* also noted that Chinese law does not

[30] *See Public Safety and Homeland Security Bureau Seeks Comment on the June 9, 2020 Filing by the National Telecommunications and Information Administration in PS Dockets 19-351 and 19-352*, Public Notice, PS Docket Nos. 19-351, 19-352, DA 20-603 (PSHSB Jun. 9, 2020).

[31] *See generally* Huawei NTIA Filing Comments; NTCA – The Rural Broadband Association NTIA Filing Comments; RWA NTIA Filing Comments; USTelecom NTIA Filing Comments.

[32] *Order*, 34 FCC Rcd at 11439, para. 41.

[33] *See id*.

[34] *Order*, 34 FCC Rcd at 11438-39, para. 41.

[35] The Commission concluded in the *Order* that the record contained sufficient publicly available information to support its initial designations, and we further conclude that publicly available information in the record is sufficient to support the final designation of Huawei as a covered company as well. Nevertheless, the Commission compiled and reviewed additional classified national security information that provided further support for its initial designation. *Order*, 34 FCC Rcd at 11440, para. 43, n.124; *see also* 47 U.S.C. § 154(j) ("The Commission is authorized to withhold publication of records or proceedings containing secret information affecting the national defense."). This classified information remains a part of the record in this proceeding and provides further support for this final designation.

[36] 47 CFR § 54.9(a); *Order*, 34 FCC Rcd at 11433, para. 26. This prohibition applies to any affiliates of USF recipients to the extent that such affiliates use USF funds. *See Order*, 34 FCC Rcd at 11433, para. 26, n.77.

[37] *Order*, 34 FCC Rcd at 11433, 11439-41, paras. 27, 43-46.

meaningfully restrain the Chinese government because of that government's "authoritarian nature, lack of sufficient judicial checks, and its history of industrial espionage."[38] The Commission further cited evidence of known security risks and vulnerabilities in Huawei's equipment, which has led the U.S. and some of its allies to significantly restrict the purchase and integration of Huawei equipment and services into the communications infrastructure.[39]

12. After careful consideration of the record in this proceeding, we conclude that Huawei poses a national security threat to the integrity of communications networks and the communications supply chain. This conclusion rests on our finding that Huawei is highly susceptible to coercion by the Chinese government; the risks highlighted by U.S. policymakers and the intelligence community, as well as allied nations and communications providers; and the known security risks and vulnerabilities in Huawei's equipment. Accordingly, we issue this final designation of Huawei as a covered company for the purposes of the Commission's rule.

1. Huawei is Highly Susceptible to Influence and Coercion by the Chinese Government, Military, and Intelligence Community

13. First, we find that Huawei is susceptible to coercion, both legal and political, and this presents profound risks to the security of our nation's communications networks.[40] We find that Huawei's close ties to the Chinese government, both at the level of ownership and at the employee level, as well as its obligations under Chinese law, present far too great a risk to U.S. national security to continue to subsidize the use of Huawei equipment and services. The record of this proceeding confirms the conclusion of a recent U.S. national security advisor concerning Huawei "and its role in China's security apparatus" and specifically "the grave national security danger associated with a wide array of Huawei's telecommunications equipment."[41]

14. Our review of the record leads us to affirm the Commission's initial findings that the Chinese government is highly centralized and exercises strong control over commercial entities in its sphere of influence, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with governmental requests, including revealing customer information and network traffic information.[42] Demands for such information could come in the form of legal pressure, as in the case of the Chinese National Intelligence Law, or in the form of extra-legal political pressure taken through control of subsidy funding, employee unions, or threats and/or coercion. We agree with the Commission's finding that "state actors, . . . notably China, . . . have supported extensive and damaging cyberespionage efforts in the United States,"[43] and there exists a "substantial body of evidence" about the risks of certain equipment providers like Huawei.[44] International

---

[38] *Order*, 34 FCC Rcd at 11442-43, para. 49 n.146.

[39] *Order*, 34 FCC Rcd at 11442-44, paras. 48-58.

[40] *See Order*, 34 FCC Rcd at 11442-44, paras. 48-51.

[41] H.R. McMaster, What China Wants, *The Atlantic*, May 2020, at 74.

[42] *See Order*, 34 FCC Rcd at 11441, para. 46. *See also* 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.

[43] *Order*, 34 FCC Rcd at 11440, para. 44 (quoting TIA Comments at 10).

[44] *Order*, 34 FCC Rcd at 11440, para. 44 (quoting 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.")); *see 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).

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."[45] 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."[46]

15. We also agree with the Commission's finding that Huawei poses a particular security risk because Chinese intelligence agencies have opportunities to tamper with Huawei's products in both the design and manufacturing processes.[47] A 2012 "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE" written by the Select Committee on Intelligence of the U.S. House of Representatives (*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 this service allows it "authorized access" to the equipment and network that could be exploited "for malicious activity under the guise of legitimate assistance."[48] As the U.S. Attorney General has argued in this proceeding, "a company's ties to a foreign government and willingness to take direction from it bear on its reliability" for building or servicing telecommunications networks with the support of federal funds.[49]

16. We find unpersuasive Huawei's contention that the Commission acted arbitrarily and capriciously by selectively targeting Huawei and ZTE while ignoring other companies which Huawei claims are similarly situated.[50] The Commission acted in November 2019 based on the evidence in the

[45] *Order,* 34 FCC Rcd at 11440, para. 44 (quoting 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)).

[46] *Order*, 34 FCC Rcd at 11440, para. 44 (quoting RWR 2019 Report at 8).

[47] *See Order*, 34 FCC Rcd at 11440-41, para. 45. *See also HPSCI Report* at 3 (observing that during product development, "malicious hardware or software [could be] implant[ed] into critical telecommunications components and systems").

[48] U.S. House of Representatives, Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE at 3-4 (2012) (*2012 HPSCI Report*); *see Order*, 34 FCC Rcd at 14440, para. 45. This report contains the findings of an investigation initiated in 2011 by the House Permanent Select Committee on Intelligence "to inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States." *2012 HPSCI Report* at iv. The Committee ultimately concluded that the "failure of [Huawei and ZTE] to provide responsive answers about their relationships with and support by the Chinese government provides further doubt as to their ability to abide by international rules." *Id.* at 44. Huawei argues at length that the *2012 HPSCI Report* is both "untrustworthy and unreliable" as a source of evidence. Huawei Comments at 62-64. We do not, however, accept uncritically all of the findings of this report. We do, however, note the findings of that report were the product of a detailed and lengthy investigation. We further note that the findings of this report cited herein are corroborated by other sources, which were both cited and discussed in the Commission's initial designated and which are likewise discussed herein. And so, even if the *2012 HPSCI Report* is not considered conclusive evidence, it is among the broad range of evidence that the Commission may appropriately consider in making its designation. *See, e.g.*, *Holy Land Foundation for Relief & Development v. Ashcroft*, 333 F.3d 156, 162 (2003) (explaining that, under the International Emergency Economics Power Act , "it is clear that the government may decide to designate an entity based on a broad range of evidence, including intelligence data and hearsay declarations"); *People's Mojahedin Org. of Iran v. U.S. Dep't of State*, 182 F.3d 17, 19 (D.C.Cir.1999) (noting that "nothing in the legislation [at issue] restricts [the Department of State] from acting on the basis of third hand accounts, press stories, material on the Internet[,] or other hearsay regarding the organization's activities").

[49] *See Order*, 34 FCC Rcd at 11440-41, para. 45; 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.").

record that demonstrated overwhelmingly that both Huawei and ZTE should be considered harmful to the country's telecommunications network security, and any effort by Huawei to point at other allegedly similarly situated companies ignores that record evidence. We take the same approach as the House Permanent Select Committee on Intelligence, which, in discussing its choice to initially focus its investigation on Huawei and ZTE, explained, "[t]hese may not be the only two companies presenting [a] risk, but they are the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United States."[51] Even if other companies may warrant further investigation, the Commission has chosen to proceed incrementally by first initially designating Huawei and ZTE before investigating other companies that may pose potential threats.[52]

17. *Huawei's close ties to the Chinese Government and military make it susceptible to political and economic coercion.* Huawei has close ties to the Chinese government and the Chinese military making Huawei susceptible to extra-legal, coercive pressure from Chinese military and intelligence agencies.[53] Huawei acknowledges that Huawei Technologies USA, Inc. is a subsidiary of Huawei Technologies Co., Inc., which is in turn owned by Huawei Investment & Holding Co., Ltd. (Huawei Investment & Holding).[54] Because these companies are not publicly traded, their corporate governance and ownership are largely not public. Huawei Investment & Holding has two shareholders. One is Ren Zhengfei, Huawei's founder, who owns one percent of shares.[55] According to reports, the other shareholder is the Union of Huawei Investment & Holding, Huawei's labor union, which owns the remainder of shares.[56] The full weight of the union's financial and other influence is unclear, including the influence of the government within the trade union, because Huawei is not publicly traded and has never allowed an independent review of its ownership structure.[57] At a minimum, the Chinese Communist Party treats Huawei as a state-owned enterprise, and it has benefited from procurements funds, subsidized funding, and state funding for research.[58] Given the Chinese Communist Party's heavy influence in similarly situated enterprises, we are not persuaded that the government does not hold similar influence here.[59]

18. Huawei also has demonstrably close ties to the Chinese military. Among Huawei employees in the Union, there are "key mid-level technical personnel" with backgrounds in work closely associated with intelligence gathering and military activities, specifically with the People's Liberation Army and the Ministry of State Security, which directs China's counter-intelligence, foreign intelligence, and political security activities.[60] Huawei concedes that its founder, Ren Zhengfei, previously served as a

(Continued from previous page)

[50] *See* Huawei Comments at 105-14.

[51] *2012 HPSCI Report* at 8.

[52] *See Advocates for Highway & Auto Safety v. Fed. Motor Carrier Safety Admin.*, 429 F.3d 1136, 1147 (D.C. Cir. 2005) ("Agencies surely may, in appropriate circumstances, address problems incrementally.").

[53] *See Order*, 34 FCC Rcd at 11440-41, para. 45.

[54] Huawei Comments at 4-5, 43.

[55] Huawei Comments at 5, 43.

[56] Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated.*, New York Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html; *see also* Huawei Comments at 5, 43 (stating that Huawei Investment & Holding Co. is owned by Zhengfei and employees "through an employee stock ownership plan").

[57] 2012 HSPCI Report at 13-20.

[58] NTIA Letter at 7. *See also Order*, 34 FCC Rcd 11443, para. 51 (citing RWR Report at 4 (noting that Huawei is treated as a state-owned enterprise and has benefited from procurement funds, subsidized financing from state-owned banks and state funding for research)).

[59] *See id.*

Deputy Director in the Civilian Engineering Corps of the People's Liberation Army.[61] In addition to his one percent ownership of shares, Huawei acknowledges that its charter provides Zhengfei with certain veto powers, "including the right to veto amendments to governance documents or to veto increases or decreases in the registered capital of Huawei."[62]

19. Moreover, Huawei benefits from vast subsidies from the Chinese government, including state-controlled financial organizations, through lucrative project funding and lines of credit extended to foreign companies to incentivize the purchase of Huawei products.[63] We agree with NTIA, which argues that "the fact that maintaining a good relationship with the [Chinese Communist Party] is a prerequisite for business success has led companies like Huawei to be active participants in achieving the goals of the State."[64] Other experts have also recognized "the integrated nature of the Chinese Communist Party's military and economic strategies," across "government, industry, academia, and the military," and its ability "to induce cooperation, wittingly or unwittingly, from . . . companies."[65] This corporate legal structure, tied as it is to elements of the Chinese military and intelligence apparatus, further leads us to the conclusion that Huawei is highly subject to coercive pressure from the Chinese government and, therefore, presents an untenable risk to U.S. national security given the critical infrastructure role of U.S. communications networks.[66]

20. Huawei's observation that all companies operating in China, including foreign-owned companies, must have internal Communist party committees does not alleviate our concerns regarding the Chinese Communist Party's ability to exert pressure over Huawei.[67] Indeed, we agree that many Western companies have complained about their Chinese affiliates "being 'guided' by party committees," and that "the [Chinese Communist Party] has the intention to influence and to use party committees or cells in at

(Continued from previous page)

[60] Christopher Balding, Huawei Technologies' Links to Chinese State Security 1 (Jul. 5, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726. *See also* Isobel Asher Hamilton, *Researchers studied 25,000 leaked Huawei resumes and found troubling links to the government and spies*, Business Insider (Jul. 8, 2019), https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7.

[61] Huawei Comments at 132.

[62] Huawei Comments at 133.

[63] RWR Advisory Group, A Transactional Risk Profile of Huawei, at 20 (Feb. 2018), https://www.rwradvisory.com/wp-content/uploads/2018/04/RWR-Huawei-Risk-Report-2-13-2018.pdf. 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)." *Id*. at 21. 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. *Id*. Although Huawei denies that the subsidies it receives from the Chinese government are "vast" when "compared to Huawei's revenues and expenditures," Huawei Comments at 84, it does not provide any quantification of the financial support it receives that would allow for an independent assessment of this claim.

[64] NTIA Letter at 7. The Executive Branch notes that, as an example of Huawei's participation with Chinese state oppression, Huawei has supported the Chinese government's surveillance and detention of over a million Uighurs, depriving them of their freedom and their human rights. *See id*.

[65] H.R. McMaster, What China Wants, *The Atlantic,* May 2020, at 70, 71, 73. For example, General McMaster notes, Chinese cybertheft, including use of a hacking squad by the Ministry of State Security, has been responsible for what the former director of the NSA describes as the "greatest transfer of wealth in history." *Id.* at 73 (quoting General Keith Alexander).

[66] *See* NTIA Letter at 8 ("As long as Huawei and ZTE are subject to the legal and extralegal influence and control of the Chinese government and the [Chinese Communist Party], there are doubts that the companies can be trusted to comply fully with U.S. law . . . Huawei has allegedly offered bonuses to its employees based on the value of information they stole from other globally-situated companies.").

[67] Huawei Comments at 43-44.

least some instances.'"[68] But a Chinese-headquartered company would be even more susceptible to Chinese government pressure than a Chinese affiliate of a non-Chinese company.[69] Moreover, we find that the Chinese government's coercive power over Chinese technology companies seems to be increasing, as the U.S.-China Economic and Security Review Commission found in November 2019 that "after years of thriving under light regulation," "[i]n recent months, China's technology sector has faced stepped-up government scrutiny and increased pressure to align with Party edicts."[70]

21. *Huawei's obligations under Chinese national intelligence laws obligate it to assist with Chinese military and intelligence agency requests.* In an effort to bolster its own national security interests, the Chinese government has taken a highly centralized and commanding approach to exercise strong control over commercial and economic enterprises through enactment of the Chinese National Intelligence Law , effective in June 2017 and revised in April 2018.[71] Huawei, as a Chinese-owned company, is subject to the Chinese National Intelligence Law which compels it to assist the Chinese government in espionage activities. The Chinese National Intelligence Law "entrenched the already unwritten understanding that Chinese companies and their employees are required to comply with government orders in the area of national intelligence work."[72] Because of China's "notorious reputation for persistent industrial espionage," particularly involving close collaboration between the Chinese government and Chinese industry,[73] we find that, even if the Chinese National Intelligence Law could be interpreted in more benign ways, the legal risks that the law poses support a finding that Huawei equipment and services pose a national security threat. As a former U.S. national security advisor has concluded, the Chinese National Intelligence Law as amended effectively "declared that all Chinese companies must collaborate in gathering intelligence."[74]

22. A close reading of the provisions of the Chinese National Intelligence Law demonstrates that it is broad enough to allow the Chinese government to compel Chinese companies such as Huawei to assist it in its espionage activities. Article 7 of the Chinese National Intelligence Law on its face obligates "all organizations and citizens" to "support, assist, and cooperate with national intelligence efforts in accordance with law" and to "protect national intelligence work secrets" without any apparent limitation on the type of assistance the Chinese government may demand.[75] In a similar vein, Article 14 of the

---

[68] RWR 2019 Report at 26 (quoting Chinese telecommunication companies: Political and legal vulnerabilities and how Europe should deal with them, Mercator Institute for China Studies, March 13, 2019).

[69] For example, Google closed its Chinese search engine after facing pressure from the Chinese government to censor search results, a strategy likely unavailable to a Chinese-headquartered company. Steve Lohr, *Interview: Sergey Brin on Google's China Move*, New York Times (Mar. 22, 2010), https://bits.blogs.nytimes.com/2010/03/22/interview-sergey-brin-on-googles-china-gambit/.

[70] 2019 Report to Congress, U.S.-China Economic and Security Review Commission, at 135 (Nov. 2019), https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.

[71] *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 (citing to an interrelated package of national security, cyberspace, and law enforcement legislation "aimed at strengthening the legal basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them").

[72] RWR 2019 Report at 23.

[73] 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). *See also* McMaster, *supra,* at 73.

[74] H.R. McMaster, What China Wants, *The Atlantic*, May 2020, https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/.

[75] Chinese National Intelligence Law, Article 7; *see also* Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities (2019).

Chinese National Intelligence Law allows Chinese intelligence institutions to request that Chinese citizens and organizations provide necessary support, assistance, and cooperation, while Article 17 permits those intelligence institutions to commandeer an organization's facilities, including communications equipment.[76] The applicability of the law to "all organizations and citizens," coupled with a lack of geographic limitation in scope, suggests, by a literal interpretation, an "unusually broad scope of application."[77] Furthermore, the absence of a definition of "organization" in the Chinese National Intelligence Law indicates a broad interpretation of the term, conceivably extending the law to encompass an individual business incorporated in China or a group of entities, enveloping a parent company headquartered in China as well as the parent's foreign subsidiaries.[78] In fact, Article 11 of the Chinese National Intelligence Law specifies that Chinese state intelligence entities may launch intelligence initiatives both within and beyond Chinese borders.[79] As the Executive Branch has explained in the record, "[t]aken together, these laws empower the People's Republic of China government to make extensive, affirmative demands on Chinese companies and their officers and employees to advance the [Chinese Communist Party's] intelligence gathering interests."[80] We therefore conclude that the Chinese National Intelligence Law, through its broad application, could reasonably permit the Chinese government and its intelligence agencies to compel Huawei Technologies USA, as a foreign subsidiary of a corporation headquartered in China, to carry out its directives in cyberespionage or other actions contrary to U.S. national security interests.

23. Huawei contends that the Chinese National Intelligence Law does not permit the Chinese government to compel companies such as Huawei to spy for it.[81] But such a reading is clearly not required by the text—precisely where one might expect such a law to be specific to support a limited reading, it is instead vague. And even if Huawei interprets the law in a more narrow fashion, it cannot so bind the Chinese government and we would nonetheless find a significant risk of collaboration between Huawei and Chinese military and intelligence services given Huawei's close connections to the Chinese government and those entities.[82]

---

[76] Chinese National Intelligence Law, Articles 14 and 17; *see also* 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.

[77] Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities at 2-3 (2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf (observing that the Chinese National Intelligence Law lacks language found in comparable Chinese security laws, the National Security Law and the Cyber Security Law, which delimits the application of the Chinese National Intelligence Law to "citizens residing in the territory of China, companies established in China or activities performed on Chinese territory"). *See also* 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 (stating the Chinese National Intelligence Law "leaves key concepts undefined, thereby expanding the law's potential scope and its risks to foreigners").

[78] 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.

[79] Chinese National Intelligence Law, Article 11; 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 23 (May 2019), https://www.rwradvisory.com/wp-content/uploads/2019/05/Assessing-Huawei-Risk.pdf (RWR 2019 Report).

[80] NTIA Letter at 5.

[81] *See* Huawei Comments at 92-105; Huawei NTIA Filing Comments at 2.

[82] *See* NTIA Letter at 5 ("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 [Chinese Communist Party].")

24. Nor are we convinced by Huawei's submissions purporting to show that, regardless of any applicable law, Huawei would refuse any government request for customer data.[83] This is because any resistance by Huawei to requests for assistance by Chinese intelligence services would likely be futile in light of the Chinese government's authoritarian nature, lack of sufficient judicial checks, and its history of industrial espionage.[84] Indeed, the Chinese law expert on whom Huawei relies in attempting to rebut these allegations concedes that his opinion is provided solely from his own legal perspective and does not take into account political realities.[85] Despite Huawei's claims of independence, other experts irrevocably contradict his argument. New York University Law Professor Jerome Cohen has stated that "'[t]here is no way Huawei can resist any order from the (People's Republic of China) or the Chinese Communist Party to do its bidding in any context, commercial or otherwise.'"[86] The Executive Branch has also determined that Chinese law imposes "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," and "provides no ability, check, or balance for companies or individuals to refuse these requests."[87] We credit the analysis by the expert agencies of the Executive Branch of the U.S. government, particularly their explanation of how companies such as Huawei are beholden to the legal and extralegal controls of the Chinese government and Chinese Communist Party.[88]

25. Although Huawei points to the possibility of "judicial relief" as a method for aggrieved companies like Huawei to protest excessive or extra-legal demands from the Chinese government,[89] we have little confidence that Chinese courts have sufficient independence from the Chinese Communist Party to allow them to render impartial interpretations of the Chinese National Intelligence Law.[90] Indeed, Zhou Qiang, Chief Justice and President of the Supreme People's Court of China, has cautioned that Chinese courts "'must firmly resist the western idea[s] of 'constitutional democracy,' 'separation of powers,' and 'judicial independence.'"[91] As the Executive Branch points out, "one of the conditions for becoming a judge is 'supporting . . . the leadership of the Communist Party of China and the socialist

[83] *See* Huawei Comments at 44-46.

[84] *Order*, 34 FCC Rcd at 11442-43, para. 49 n.146.

[85] 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); *see Order*, 34 FCC Rcd at 11442-43, para. 49 n.147.

[86] Finite State, Finite State Supply Chain Assessment at 7 (2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf (Finite State Supply Chain Report) (quoting Prof. Cohen).

[87] NTIA Letter at 5. As noted above, General McMaster has reached a similar conclusion, in identifying "incontrovertible evidence of the grave national-security danger associated with a wide array of Huawei's telecommunications equipment." *See* H.R. McMaster, What China Wants, *The Atlantic*, at 74 (May 2020).

[88] NTIA Letter at 4-8. We note that the Commission has historically found it appropriate to seek and accord deference to the expressed views of the Executive Branch in identifying and interpreting issues of national security, law enforcement, and foreign policy. *See Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, Report and Order and Order on Reconsideration, FCC 97-398, 12 FCC Rcd 23891, 23919, para. 63 (1997); *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, FCC 19-38, 34 FCC Rcd 3361, 3362-63, para. 2 (2019).

[89] Huawei Comments at 105.

[90] *See* NTIA Letter at 6 ("The Chinese judiciary also lacks the independence and power to check the demands of the government or the [Chinese Communist Party].").

[91] RWR 2019 Report at 21-22 (quoting Qiang).

system.'"[92] We likewise have little confidence in Huawei's intent to seek such judicial relief given its prior experience with assisting foreign governments in spying.[93]

26. Moreover, in the unlikely event that Huawei's leadership were to resist the Chinese government's attempts at coercion, the *2012 HPSCI Report* underscores that "Chinese intelligence services need only recruit working-level technicians or managers" to perform the bidding of the intelligence or military agencies without having to involve Huawei's leadership.[94] Furthermore, recruiting such low-level and mid-level employees would likely be successful, because in China, "[i]ndependent oversight bodies over state security organs that citizens and enterprises might turn to if they receive undue requests for cooperation are de facto non-existent."[95] Researchers have already found strong evidence that key technical personnel employed by Huawei have experience and backgrounds that encourage close cooperation with intelligence gathering and military activities.[96]

27. Huawei's susceptibility to both legal and political forms of pressure to participate in Chinese government espionage, along with China's proven history of partnering with its industry to engage in such espionage supports our conclusion that Huawei poses a national security threat to the integrity of the nation's communications networks and the communications supply chain.

2. Designation of Huawei Aligns with the Findings and Actions of Congress, the Executive Branch, United States Policymakers, the Intelligence Community, Allied Nations, and Communications Providers

28. As with the Commission's initial designation of Huawei as a covered company, our determination today is guided in part by the national security risks and concerns that have led the United States and its allies to take steps towards protecting and securing communications infrastructure and the supply chain from Huawei.[97] Here in the United States, both the executive and the legislative branches have moved to limit the deployment and impact of Huawei equipment and services, while foreign allies and providers in other countries have also taken steps to restrict such equipment and services.

29. We acknowledge and are informed by legislative and Presidential action, such as when 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."[98] Similarly, in 2018, Congress passed, and the President signed into law, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA),[99] which prohibits executive agencies from obligating or expending loan or grant funds to

[92] NTIA Letter at 6. The Executive Branch also notes that the Chinese Communist Party also appoints, dismisses, transfers, and promotes judges and that courts fall under the jurisdiction of local governments, which also control the courts' budgets. *Id*.

[93] Joe Parkinson, Nicholas Bariyo, and Josh Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, Wall Street Journal (Aug. 15, 2020), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[94] *2012 HPSCI Report* at 3.

[95] RWR 2019 Report at 27 (quoting MERICS report).

[96] Christopher Balding, Huawei Technologies' Links to Chinese State Security, at 1 (Jul. 5, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726. *See also* Isobel Asher Hamilton, *Researchers studied 25,000 leaked Huawei resumes and found troubling links to the government and spies*, Business Insider (Jul. 8, 2019), https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7.

[97] *See Order*, 34 FCC Rcd at 11444, paras. 52-53.

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

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.[100] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services," as relevant here, as telecommunications equipment produced by Huawei or ZTE or any subsidiary or affiliate of such entities.[101] Moreover, the recent passage on March 12, 2020 of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act) reflects the U.S. government's ongoing concern that Huawei's equipment poses a national security risk.

30. We are also bolstered in our decision by other agencies and branches of government, having studied the risks of permitting equipment and services from Huawei into the U.S. telecommunications network, and with access to additional information and policy expertise, have seen fit to take these actions notwithstanding the burdens they may impose on the U.S. economy. The actions of U.S. Executive Branch agencies also reflect heightened concerns over the risk to national security from the continued use of Huawei equipment and services.[102] For example, 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, that the entity has been involved, is involved, or poses a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States."[103] Moreover, 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 Christopher Wray saying, "we are 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."[104]

31. Our decision is further informed by similar risk assessments conducted by many of the United States' allies, which have resulted in numerous countries restricting the purchase or integration of Huawei equipment and services into network infrastructure. For example, Australia and Japan have concluded that Huawei poses a security risk and have taken steps to exclude Huawei equipment from their domestic communications systems.[105] Although the European Union has decided not to explicitly ban Huawei from its 5G networks, it has adopted strict guidelines for vetting 5G equipment vendors, "allow[ing] EU capitals to limit Huawei's role in 5G networks across the Continent in coming years."[106]

(Continued from previous page)

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

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

[101] *See* Pub. L. 115-232, 132 Stat. 1918, § 889(f)(3)(A) (2019 NDAA).

[102] *See* NTIA Letter at 1 (expressing the Executive Branch's support for designating Huawei and ZTE).

[103] 15 CFR § 744.11(b); *see* 15 CFR Part 744, Supp. 4 (Entity List).

[104] *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#.

[105] *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; 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.

[106] Laurens Cerulus, *Europe's Huawei plan explained*, Politico Europe (Jan. 29, 2020), https://www.politico.eu/article/europe-eu-huawei-5g-china-cybersecurity-toolbox-explained/. Helene Fouquet and Natalia Drozdiak, *EU Won't Recommend Banning Huawei in Upcoming 5G Risk Rules*, Bloomberg (Jan. 20, 2020), https://www.bloomberg.com/news/articles/2020-01-20/eu-won-t-recommend-banning-huawei-in-upcoming-5g-risk-rules.

Within the EU, while no government has yet imposed an outright ban on Huawei products or services, many are in the throes of deliberation.[107] Additionally, Canada, New Zealand, Italy, Germany, the Netherlands, the United Kingdom, and others are currently assessing whether to ban Huawei technology from their networks.[108]

32. Moreover, communications providers in a number of countries have already set forth their own initiatives to limit or cease business dealings with Huawei altogether, with major providers cutting Huawei from their mobile phone offerings, network cores, and future 5G network builds.[109] For example, BT, Orange, and Deutsche Telekom are acting to keep Huawei equipment out of their 5G networks.[110] It is telling that European telecom operators, themselves Huawei customers, are actively working to remove Huawei's equipment from their core networks.[111] In Greenland, Norway, and Poland, nationwide telecom operators have partnered with competitors to Huawei to serve as vendors in 5G deployment.[112] These actions taken by the telecommunications industry to limit Huawei's integration into the supply chain, driven by telecommunications providers' own assessments of the exposure to risk within their own networks, indicate that the security vulnerabilities present in Huawei's equipment should not be taken lightly.

33. We understand that some foreign governments have declined to ban all Huawei equipment and services from their national communications infrastructure and communications supply chain and Huawei encourages us to consider these refusals as we determine whether to designate it.[113]

---

[107] Reuters, *Explainer: As Britain Decides, Europe Grapples with Huawei Conundrum*, New York Times (Jan. 22, 2020), https://www.nytimes.com/reuters/2020/01/22/business/22reuters-europe-usa-huawei-explainer.html.

[108] *See* Stu Woo, *Facing Pushback from Allies, U.S. Set for Broader Huawei Effort*, Wall Street Journal (Jan. 23, 2020), https://www.wsj.com/articles/facing-pushback-from-allies-u-s-set-for-broader-huawei-effort-11579775403; B. Lana Guggenheim, *Questions Over Cyber Security Cause Uncertainty in Europe*, South EU Summit (Jan. 9, 2020), https://www.southeusummit.com/europe/questions-over-cyber-security-cause-uncertainty-in-europe/; Reuters, *Explainer: As Britain Decides, Europe Grapples with Huawei Conundrum*, New York Times (Jan. 22, 2020), https://www.nytimes.com/reuters/2020/01/22/business/22reuters-europe-usa-huawei-explainer.html; Mary-Ann Russon, *Fresh UK review into Huawei role in 5G networks*, BBC (May 24, 2020), https://www.bbc.com/news/business-52792587.

[109] *See* Shannon Liao, *Verizon won't sell Huawei phones due to US government pressure, report says*, The Verge (Jan. 30, 2018), https://www.theverge.com/2018/1/30/16950122/verizon-refuses-huawei-phone-att-espionage-cybersecurity-fears; Sean Keane, *BT to strip Huawei equipment from 4G network by 2021, won't use it in 5G core*, CNET (Dec. 5, 2018), https://www.cnet.com/news/bt-to-strip-huawei-equipment-from-4g-network-by-2021-wont-use-it-in-5g-core/; Victoria Klesty, Terje Solsvik, *Norway's Telenor picks Ericsson for 5G, abandoning Huawei*, Reuters (Dec. 13, 2019), https://www.reuters.com/article/us-telenor-ericsson-huawei-tech/norways-telenor-picks-ericsson-for-5g-abandoning-huawei-idUSKBN1YH0RM; Pavel Alpeyev and Takahiko Hyuga, *Huawei Loses a Key Customer for 5G Network*, Bloomberg (May 29, 2019), https://www.bloomberg.com/news/articles/2019-05-29/huawei-loses-a-key-customer-as-softbank-opts-for-5g-alternatives?srnd=technology-vp.

[110] NATO Cyber Defence Centre Paper at 17.

[111] Reuters, *Explainer: As Britain Decides, Europe Grapples with Huawei Conundrum*, New York Times (Jan. 22, 2020), https://www.nytimes.com/reuters/2020/01/22/business/22reuters-europe-usa-huawei-explainer.html.

[112] Reuters, *Factbox: Deals by Major Suppliers in the Race for 5G*, New York Times (Jan. 13, 2020), https://www.nytimes.com/reuters/2020/01/13/business/13reuters-telecoms-5g-orders.html.

[113] *See* Huawei Comments at 51-53; Natasha Lomas, *UK will allow Huawei to supply 5G – with 'tight restrictions'*, TechCrunch (Jan. 28, 2020), https://techcrunch.com/2020/01/28/uk-will-allow-huawei-to-supply-5g-with-tight-restrictions/; Hadas Gold, *UK will allow Huawei to help build its 5G network despite US pressure*, CNN Business (Jan. 28, 2020), https://www.cnn.com/2020/01/28/tech/huawei-5g-uk/index.html; William Booth, Jeanne Whalen, and Ellen Nakashima, *Britain, resisting U.S. pressure, to allow some Huawei equipment in 5G networks*, Washington Post (Jan. 28, 2020), https://www.washingtonpost.com/world/europe/britain-resisting-us-pressure-to-allow-some-huawei-equipment-in-5g-networks/2020/01/28/52e708b4-4145-11ea-99c7-1dfd4241a2fe_story.html.

Ultimately, we are not persuaded by these other countries to use our own federal funding—which comes from fees paid by American consumers and businesses—for Huawei equipment or services. Just as each sovereign nation may reach its own determination regarding the integration of products that may threaten national security, we conduct our own assessment of the risks associated with Huawei's products and services in light of the record and information pertinent to the United States and its national interests.[114] We also note that several countries that have decided against an outright ban of Huawei products at this time have also limited the role Huawei will play in their nation's communications supply chain.[115] For example, the United Kingdom, in restricting "high risk" vendors such as Huawei from supplying Britain's 5G network, initially decided to permit Huawei to build "non-core" 5G infrastructure, yet to exclude its equipment in safety-critical and sensitive network infrastructure and will cap its market share at 35%.[116] The United Kingdom is now considering further restrictions on Huawei's role in 5G networks.[117]

3. Huawei's Equipment Contains Known Security Risks and Vulnerabilities

34. Our determination in this case is further supported by evidence that the security risk to our communications networks from permitting USF funds to be used for the purchase of Huawei equipment and services is significant.[118] In 2019, a cybersecurity firm, Finite State, reported hundreds of vulnerabilities identified in Huawei firmware, including the presence of backdoors that potentially could be used to allow an attacker with knowledge of the firmware to log into the device.[119] Finite State found that "[i]n virtually all categories," Huawei devices were "less secure than comparable devices from other vendors."[120] Nevertheless, according to Finite State, "Huawei has repeatedly failed to address these vulnerabilities when making firmware updates."[121] We find that the Finite State Report substantiates the Commission's concerns regarding the weak security culture at Huawei. We disagree with Huawei's criticisms of the report, but even if the report is flawed in some respects, "Huawei cannot deny that, now, multiple organizations have independently found similar, substantial security vulnerabilities in their products."[122]

35. Although Huawei asserts that there is no evidence it has ever planted spyware in its equipment,[123] there are in fact reports of alleged espionage conducted on Huawei's networks. In Uganda

---

[114] *See Order*, 34 FCC Rcd at 11444, para. 53 n.160 ("[W]e 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.").

[115] *See, e.g.*, Press Release, U.K. Department for Digital, Culture, Media & Sport, et al., New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity, (Jan. 28, 2020), https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity; Helene Fouquet and Natalia Drozdiak, *EU Won't Recommend Banning Huawei in Upcoming 5G Risk Rules*, Bloomberg (Jan. 20, 2020), https://www.bloomberg.com/news/articles/2020-01-20/eu-won-t-recommend-banning-huawei-in-upcoming-5g-risk-rules.

[116] *See* William Booth, Jeanne Whalen, and Ellen Nakashima, *Britain, resisting U.S. pressure, to allow some Huawei equipment in 5G networks*, Washington Post (Jan. 28, 2020).

[117] *See* Mary-Ann Russon, *Fresh UK review into Huawei role in 5G networks*, BBC (May 24, 2020), https://www.bbc.com/news/business-52792587.

[118] *See Order*, 34 FCC Rcd at 11145-47, paras. 54-57.

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

[120] Finite State Report at 2.

[121] Finite State Report at 3.

[122] *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.

[123] *See* Huawei Comments at 89.

and Zambia, where Huawei equipment dominates the communications market, Huawei employees aided African governments to spy on political opponents.[124] A newspaper investigation uncovered how the Huawei technicians personally and expeditiously hacked encrypted communications using Huawei technology and other products, after government security officials failed to intercept the communications on their own.[125]

36. The United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board (Oversight Board) has also documented the risks associated with Huawei's engineering processes.[126] The Oversight Board stated in its 2019 report that it "has continued to identify concerning issues in Huawei's approach to software development bringing significantly increased risk to UK operators," observing that "[n]o material progress ha[d] been made on the issues raised in the previous 2018 report."[127] As a result, "[t]he Oversight Board continues to be able to provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK," and it will be difficult for the Oversight Board "to appropriately risk-manage future products in the context of UK deployments, until the underlying defects in Huawei's software engineering and cyber security processes are remediated."[128] It is therefore no surprise that the United Kingdom has banned Huawei from the core of 5G networks.

37. Telecommunications companies that use equipment manufacturers to construct their networks have identified vulnerabilities in Huawei's equipment, which have in turn impacted whether such companies continue do business with Huawei. For example, during routine independent security testing, European carrier Vodafone discovered vulnerabilities in equipment supplied by Huawei as far back as 2011.[129] While Vodafone did not find evidence of unauthorized access and claimed that the software issues were resolved by Huawei in 2011 and 2012, testing revealed that security vulnerabilities remained even after assurances from Huawei that they had been addressed.[130]

38. We are also persuaded by concerns that Huawei's broad range of equipment, products, and services generate data on an enormous scale, concentrating information gathered from diverse platforms and systems in the hands of one company.[131] As explained in the *2012 HPSCI Report*, Huawei has a "desire to be an end-to-end provider for whole network solutions,"[132] and when companies "seek to

---

[124] Joe Parkinson, Nicholas Bariyo, and Josh Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, Wall Street Journal (Aug. 15, 2019), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[125] Joe Parkinson, Nicholas Bariyo, and Josh Chin, *Huawei Technicians Helped African Governments Spy on Political Opponents*, Wall Street Journal (Aug. 15, 2019), https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

[126] U.K. Huawei Cyber Security Evaluation Center, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (UK HCSEC Report).

[127] UK HCSEC Report at 4.

[128] UK HCSEC Report at 4.

[129] Sean Keane, *Vodafone found hidden backdoors in Huawei equipment, says report*, CNET (Apr. 30, 2019), https://www.cnet.com/news/british-carrier-vodafone-found-hidden-backdoors-in-huawei-equipment-says-report/; BBC News, *Vodafone denies Huawei Italy security risk* (Apr. 30, 2019), https://www.bbc.com/news/business-48103430.

[130] *See* Daniele Lepido, *Vodafone Found Hidden Backdoors in Huawei Equipment*, Bloomberg (Apr. 30, 2019), https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment; Sean Keane, *Vodafone found hidden backdoors in Huawei equipment, says report*, CNET (Apr. 30, 2019), https://www.cnet.com/news/british-carrier-vodafone-found-hidden-backdoors-in-huawei-equipment-says-report/.

[131] *See Order*, 34 FCC Rcd 11446, para. 56.

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."[133] We thus agree with the Commission's concern that despite its location outside of China, given the pervasive threat of the Chinese government and military apparatus, Huawei's U.S. subsidiary may be coerced to act as an extension of the intelligence-gathering arm of the Chinese state.[134] As a result, the vast amounts of data gathered by Huawei through its networks and communications equipment in the United States are essentially at risk of falling in the hands of the Chinese government.

39. Finally, we disagree with Huawei's arguments that the Finite State report should be discredited because Finite State evaluated outdated versions of Huawei's equipment,[135] did not follow general practices used for security testing, and failed to engage in dialogue with Huawei about vulnerabilities it identified.[136] Such arguments about specific vulnerabilities do not negate the conclusions of that report, much of which faults the overall approach to security at Huawei.[137] Finite State's bleak assessment of Huawei's security practices reveals a corporate culture that would extend to Huawei's entire product line.[138] Although Huawei claims the alleged backdoors uncovered by Vodafone referred to in Finite State report were fully resolved,[139] Finite State's report explained that "further testing revealed that the security vulnerabilities remained."[140] Huawei's failure to fully address vulnerabilities that are brought to its attention demonstrates its lack of commitment to secure practices, or potentially a more malicious intent. In addition, although Huawei asserts that none of its products tested by Finite State will be deployed for 5G Radio Access Network or the core in telecommunications networks, the poor security practices and corporate culture revealed by the Finite State report will carry over to the products that *are* deployed in 5G networks. We thus agree with Finite State that Huawei's "approach to security is insufficient," and that its "security posture has not materially improved over time."[141] As Finite State notes, "Huawei cannot deny that, now, multiple organizations have independently found similar, substantial security vulnerabilities in their products."[142] The Finite State report serves to substantiate the

(Continued from previous page)

[132] *2012 HPSCI Report* at 47, n.22. *See also Order*, 34 FCC Rcd at 11446, para. 56.

[133] *2012 HPSCI Report* at 2. *See also Order*, 34 FCC Rcd at 11446, para. 56.

[134] *See Order*, 34 FCC Rcd 11446, para. 56 (expressing the Commission's concern about Huawei's desire to limit diversity in the equipment market and arguing that "[t]he 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").

[135] *See* Huawei Comments at 27-28; 79. In fact, Finite State noted that its 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." 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.

[136] *See* Huawei Comments at 79; *Order*, 34 FCC Rcd at 11447, paras 57-58.

[137] *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.

[138] *See Order*, 34 FCC Rcd at 11445, para. 54.

[139] Huawei Comments at 79.

[140] Finite State Report at 5.

[141] 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.

[142] *Id*.

Commission's concern that the security culture at Huawei is weak and, therefore, products that emerge from Huawei's development environment cannot be trusted.[143] We reaffirm that conclusion here.

B. The Secure and Trusted Communications Networks Act of 2019 Demonstrates Both the Legislative and Executive Branches' Ongoing Concerns About Huawei Equipment

40. Since the time the Commission issued its initial designation of Huawei, Congress has passed, and the President signed into law, the Secure Networks Act, which provides further evidence of Congress and the President's continuing concerns about the dangers that Huawei's equipment and services continue to pose to the security and integrity of U.S. communications networks.[144] Our action today designating Huawei as a covered company that poses a national security threat to our communications networks and supply chain and the resulting ban on the use of USF funds to purchase, lease, or otherwise obtain or maintain Huawei equipment, while taken pursuant to the Commission's independent authority under the Communications Act, is consistent with the Commission's new obligations under the Secure Networks Act.[145] Indeed, section 3 of the Secure Networks Act directs the Commission to "implement" a prohibition on using USF funds for covered equipment or services from, among others, Huawei.[146]

41. We disagree with Huawei's position that the Secure Networks Act is irrelevant to this proceeding aside from confirming that the Commission purportedly lacks the authority to adopt regulations that have the objective of protecting national security.[147] Rather, the Act provides further evidence that Congress and the President continue to see Huawei equipment and services as a national security threat,[148] and indeed it explicitly preserves any action the Commission has already taken that is consistent with the Act.[149]

42. We are also unpersuaded by arguments that the Secure Networks Act requires us to limit the scope of the designation.[150] First, our action today is taken pursuant to the Commission's independent authority under the Communications Act. It is, however, consistent with the Commission's new obligations under the Secure Networks Act. Section 3 of the Secure Networks Act directs the Commission to "implement" a prohibition on using USF funds for covered equipment or services from, among others, Huawei.[151] Sections 2(b)(1) and 2(c)(3) of the Secure Networks Act provide that telecommunications equipment and services produced or provided by Huawei, because they are listed in the 2019 NDAA, "pose[] an unacceptable risk to the national security of the United States or the security

[143] *See Order*, 34 FCC Rcd at 11445, para. 54.

[144] *See* Secure Networks Act § 2(c)(3) (prohibiting equipment from companies, such as Huawei, that are listed in the 2019 NDAA). *See also* USTelecom Secure Networks Act PN Comments at 2-3 (arguing that the Secure Networks Act compels a designation of Huawei).

[145] Accordingly, we reject RWA's argument that the Commission should rely solely on the Secure Networks Act for its authority to finalize the designations. *See* RWA NTIA Filing Comments at 4.

[146] *See* Secure Networks Act § 3. *See also* USTelecom Secure Networks Act PN Comments at 2 (noting that Huawei and ZTE are properly designated as manufacturers of covered equipment under the Secure Networks Act).

[147] *See* Huawei Secure Networks Act PN Comments at 3; Huawei NTIA Filing Comments at 2-4.

[148] *See* USTelecom NTIA Filing Comments at 3 (stating that the NTIA filing confirms the Executive Branch's support for the designations and that "[t]his confirmation is meaningful and necessary because it provides certainty and rigor" to the designation process).

[149] Secure Networks Act § 3(b).

[150] *See* WTA Secure Networks Act PN Comments at 2; USTelecom Secure Networks Act PN Comments at 3; Huawei NTIA Filing Comments at 3; USTelecom NTIA Filing Comments at 4.

[151] *See* Secure Networks Act § 3. *See also* USTelecom Secure Networks Act PN Comments at 2 (noting that Huawei and ZTE are properly designated as manufacturers of covered equipment under the Secure Networks Act).

and safety of United States persons."[152] And section 2(b)(2)(C) of the Secure Networks Act grants the Commission authority to place such equipment and services on a new list of covered communications equipment and services, for which federal subsidies are prohibited, if such equipment and services pose "an unacceptable risk" to the national security of the United States or security and safety of U.S. persons.[153] We therefore reject arguments that we must limit the scope of the designation to equipment that is capable of routing or redirecting user data traffic or permitting visibility into user data or packets, or capable of remotely disrupting networks.[154] As the Commission explained in adopting the rule prohibiting use of USF funds for equipment or services from companies posing a national security risk, USF funds should not be used to deploy infrastructure or provide services that undermine our national security.[155] Indeed, the Commission has announced its judgment that "the dynamic and 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," requires a complete prohibition on the expenditure of USF funds on any and all equipment and services from a covered company.[156] Noting that malware and vulnerabilities can be built directly into equipment,[157] the Commission reasoned that such a blanket prohibition is "the only reliable protection against incursions," and that anything short of a complete ban could "allow for bad actors to circumvent our prohibitions through clever engineering."[158] The Commission also found that prohibiting all equipment and services produced by a covered company would provide regulatory certainty to USF recipients, ease the implementation of the rule for USF recipients, and make the Commission's application of the rule more administrable.[159] We understand this conclusion by the Commission to mean that all USF-funded equipment and services provided by a company that has been finally designated pursuant to section 54.9 pose an unacceptable risk to national security. We find that ongoing Congressional and Executive Branch concern about Huawei equipment and services, including that reflected by the enactment of the Secure Networks Act, supports a designation of Huawei as a covered company for purposes of the Commission's rule.

C. Huawei's Procedural and Evidentiary Challenges Fail

43. *Huawei's evidentiary challenges are misplaced*. Huawei dismisses the Commission's reasons for initially designating Huawei as a national security risk as based on "non-evidence" and "unreliable evidence,"[160] but we find Huawei's challenges to be misplaced. "In assessing risks to national security, 'conclusions must often be based on informed judgment rather than concrete evidence.'"[161] Questions involving national security therefore often "'involve the exercise of a discretion demonstrably committed to the executive or legislature.'"[162] For example, the D.C. Circuit has held that the question

[152] *See* Secure Networks Act § 2(c)(3) (prohibiting equipment listed in the 2019 NDAA such as Huawei's equipment).

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

[154] *See id.* at § 2(b)(2)(A)-(B).

[155] *See Order*, 34 FCC Rcd at 11433, para. 28.

[156] *Order*, 34 FCC Rcd at 11449, paras. 67-68.

[157] *Id*. (citing Mark L. Goldstein, Director, Physical Infrastructure Issues, U.S. Government Accountability Office, Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment 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)).

[158] *Id*.

[159] *Id.* at 11449-50, para. 69.

[160] Huawei Comments at 56-81.

[161] *Olivares v. Transportation Security Admin.*, 819 F.3d 454, 466 (D.C. Cir. 2016) (quoting *Holder v. Humanitarian Law Project*, 561 U.S. 1, 34-35 (2010)).

whether, under the Antiterrorism and Effective Death Penalty Act, the terrorist activity of an organization threatens the security of the United States was committed to the Department of State's discretion.[163] Such matters are committed to the discretion of agencies with expertise in the area.[164] In answering this question, despite Huawei's arguments that statutes, Congressional reports, and agency actions do not constitute evidence, and that statements by agency heads and members of Congress are "hearsay," it is nonetheless entirely appropriate for us to look for guidance to the actions and statements of members of Congress and agencies with expertise in national security issues, as we have done here.[165]

44. Huawei's evidentiary challenges are also misplaced for another reason. The evidentiary rules and cases cited by Huawei, such as the hearsay rule, are applicable only when an agency or court is making a factual determination to aid in evaluating the lawfulness of past conduct. In such cases, to establish that particular events occurred, proof of specific facts is obviously necessary. By contrast, where the Commission makes predictive judgments, evidentiary concerns such as hearsay may bear on the weight given to a particular piece of evidence, but we can and do consider a broad range of evidence.[166] Such "predictive judgments" made by agencies with expertise in the relevant area are entitled to deference.[167] Because the Commission has deep expertise with respect to communications networks and the communications supply chain, and the Executive Branch agencies whose views are represented by NTIA in this proceeding have expertise in matters of national security and foreign policy,[168] the Commission appropriately made a predictive judgment regarding potential risks to the integrity of communications networks and the communications supply chain from Huawei's equipment and services. The evidence and argument proffered in response to the initial designation confirms that conclusion.

45. *Huawei was not denied due process prior to the initial designation.* Huawei has been given ample opportunity in this proceeding to present its case. In response to the *Notice*, Huawei filed numerous comments, reply comments, and approximately eighteen *ex partes*.[169] After considering those submissions, the Commission announced its adoption of the rule prohibiting the use of USF funds to purchase or obtain any equipment produced or provided by a covered company posing a national security threat to the integrity of communications networks or the communications supply chain and provided

(Continued from previous page)

[162] *Al-Aulaqi v. Obama*, 727 F. Supp. 2d 1, 45 (D.D.C. 2010) (quoting *El-Shifa Pharmaceutical Indus. Co. v. United States*, 607 F.3d 836, 841 (D.C. Cir. 2010)).

[163] *See People's Mojahedin Organization of Iran v. Dep't of State*, 182 F.3d 17, 23 (D.C. Cir. 1999).

[164] *See El-Shifa*, 607 F.3d at 843.

[165] *See* Huawei Comments at 57-77; *see, e.g.*, *Holy Land*, 333 F.3d at 162 (upholding government's use of "a broad range of evidence, including intelligence data and hearsay declarations," in a determination related to national security); *People's Mojahedin Org. of Iran*, 182 F.3d at 19.

[166] *See Zevallos v. Obama*, 793 F.3d 106, 112-13 (D.C. Cir. 2015) (discussing Treasury Department's use of a variety of forms of evidence, including newspaper articles and a criminal indictment, in reaching a national security designation).

[167] *See, e.g., California by and through Becerra v. Azar*, 950 F.3d 1067, 1096 (9th Cir. 2020) ("It is well-established that an agency's predictive judgments about areas that are within the agency's field of discretion and expertise are entitled to particularly deferential review, so long as they are reasonable.") (internal quotation marks omitted); *SBC Communications v. FCC*, 138 F.3d 410, 421 (D.C. Cir. 1998).

[168] The Commission has long recognized and had a practice of deferring to the expertise of these agencies on issues of national security, law enforcement, and foreign policy. *See supra* note **Error! Bookmark not defined.**.

[169] Huawei Comments, WC Docket No. 18-89 (filed June 1, 2018); Huawei Reply Comments, WC Docket No. 18-89 (filed July 2, 2018); *see, e.g.*, *Written Ex Parte Submission of Huawei,* WC Docket No. 18-89 (filed Nov. 14, 2019); *Written Ex Parte Submission of Huawei*, WC Docket No. 18-89 (filed Nov. 12, 2019); *Written Ex Parte Submission of Huawei,* WC Docket No. 18-89 (filed Nov. 8, 2019).

Huawei notice of its initial designation as a covered company. The *Order* 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 communications networks or the communications supply chain.[170] Huawei was cited repeatedly in the *Order* as having triggered Congressional concerns regarding the potential for supply chain vulnerability and the possible risks associated with certain foreign communications equipment providers. Notably, the initial designation did not find that Huawei had violated any law and had no binding effect on any party's actions.[171] Before the adoption of any order having legal consequences to Huawei, Huawei had the opportunity to file comments in response to the initial designation and availed itself of this opportunity.[172] The Bureau then released a Public Notice seeking comments on the applicability of the Secure Networks Act to Huawei's designation proceeding, and Huawei again submitted comments.[173]

46. Huawei argues that the initial designation is invalid because it was "infected" by Congressional pressure and prejudgment by the Commissioners and, as a result, Huawei was denied the due process to which it is entitled.[174] But Huawei is mistaken. Because the initial designation had no binding legal effect and did not find Huawei liable for any past violation of law, there was no "deprivation" that would entitle Huawei to due process. Only a final designation would have any legal consequences to Huawei, and Huawei has received ample opportunity to voice its opinions and affect the Commission's decisions before the issuance of this final designation.

47. Indeed, Huawei's attempt to bring a due process challenge to the initial designation makes little sense, because the initial designation is the mechanism by which the agency provides affected entities with due process.[175] The initial designation is what provided Huawei with notice of evidence in the record and the Commission's consideration of that evidence at the time, and invited Huawei to be heard on its sufficiency or any countervailing evidence before the agency reaches any final designation that could affect its legal rights. Because the Due Process Clause is implicated only upon an actual deprivation, "due process is required not before the initial decision or recommendation to terminate . . . but instead before the termination actually occurs."[176]

48. But accepting Huawei's argument would mean that if the Commission had issued an earlier round of notice before adopting the initial designation, Huawei would have been entitled to object that *that* notice should have been preceded by an even earlier round of notice and a hearing, and it could then object to that notice on the same ground, and so on without end. But the Due Process Clause requires notice and an opportunity to be heard, not endless rounds of notice and hearings; the notice

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

[171] *See Order*, 34 FCC Rcd at 11438, 11459-11463, paras. 40, 94-103.

[172] *See generally* Huawei Comments.

[173] *See generally* Huawei Secure Networks Act PN Comments.

[174] *See* Huawei Comments at 114-24.

[175] *Cf. Orton Motor, Inc. v. U.S. Dep't of Health & Human Servs.*, 884 F.3d 1205, 1215 (D.C. Cir. 2018) (discussing the FDA's use of "warning letters" to "provid[e] notice of [alleged] violations," and holding that "the mere issuance of a warning letter, absent further enforcement action . . . 'is [not] by itself sufficient to invoke the procedural protection of the Due Process Clause'").

[176] *Riggins v. Goodman*, 572 F.3d 1101, 1110 (10th Cir. 2009)

provided by the initial designation here, and the opportunity that Huawei has to be heard prior to any final designation as a covered company under the Commission's rule, fully satisfies due process.[177]

49. In any event, Huawei makes no showing that any of the Commissioners reached their initial designation decision as a result of Congressional pressure or had prejudged the outcome. As the D.C. Circuit has explained, "mere proof that [an agency official] has taken a public position, or has expressed strong views, or holds an underlying philosophy with respect to an issue in dispute cannot overcome [the presumption of an agency's official objectivity]."[178] Even if the Commission's initial focus on Huawei in this proceeding was partially influenced by concerns of members of Congress regarding the security of Huawei's equipment, and even though some of the Commissioners made public statements reflecting their own such concerns, the Chairman and Commissioners made no statements suggesting that Huawei's designation was a foregone conclusion.[179] Further, the Commission, in making its initial designation, carefully examined evidence that indicated the risk Huawei posed.[180] And we arrive at our decision today only after having reviewed a fulsome record and multiple opportunities for Huawei to provide comment.

50. Additionally, correspondence from members of Congress asking an agency to examine a subject is not itself extraneous pressure. Huawei points to a letter to the Chairman asking the Commission to review Huawei's relationship with a U.S. telecommunications provider given Huawei's potential connection to the Chinese government's espionage efforts.[181] Huawei claims that the Commission's written response to such concerns evinces pressure but cites no case law for this proposition.[182] And Congress exerted no pressure on the Commission, such as by threatening to withhold funding, to arrive at a particular outcome.[183] Indeed, holding an adjudicatory proceeding may be an appropriate response to such an inquiry.[184] Other court cases Huawei cites in support of its prejudgment arguments are inapplicable here because they involve the question of whether the decisionmaker blatantly ignored evidence before it because of personal bias, which is not the situation here.[185]

---

[177] *See, e.g.*, *Crum v. Vincent*, 493 F.3d 988, 883 (8th Cir. 2007) ("So long as one hearing will provide . . . a meaningful opportunity to be heard, due process does not require two hearings on the same issue."); *Blackout Sealcoating, Inc., v. Peterson*, 733 F.3d 688, 691 (7th Cir. 2013) ("The due process clause . . . does not require an extended to-and-fro . . . . One opportunity to respond was enough.").

[178] *United Steelworkers of America v. Marshall*, 647 F.2d 1189, 1208 (D.C. Cir. 1980).

[179] *See Antoniu v. SEC*, 877 F.2d 721, 726 (8th Cir. 1989) (SEC Commissioner's explicit statement that the SEC had decided to bar an individual from working in securities business while a proceeding to determine that issue was still pending held evidence of prejudgment).

[180] *See Order*, 34 FCC Rcd at 11442-48, paras. 47-63.

[181] *See* Huawei Comments at 116-17.

[182] Huawei Comments at 117-18.

[183] *See Volpe*, 459 F.2d at 1246 (congressperson threatened to withhold rapid-transit appropriations to the District of Columbia if the Secretary of Transportation did not approve a bridge-construction plan); *Koniag, Inc., Vill. of Uyak v. Andrus*, 580 F.2d 601, 610 (D.C. Cir. 1978) (correspondence from a congressperson, written after testimony was heard at an agency hearing, that urged a specific outcome found to have compromised the appearance of impartiality).

[184] *See ATX, Inc. v. U.S. Dep't of Transp*., 41 F.3d 1522, 1528 (D.C. Cir. 1994) ("We are concerned when congressional influence shapes the agency's determination of the merits. . . . Congressional influence on the decision to hold a hearing is unobjectionable; if anything, the decision was an appropriate response to the pressure.").

[185] *See Metro Council of NAACP v. FCC*, 46 F3d 1154, 1164-65 (D.C. Cir. 1995); *Cinderella Careers and Finishing Schools, Inc. v. FTC*, 425 F2d 583, 590 (D.C. Cir. 1970)

51. *Huawei would not be deprived of a cognizable property or liberty interest*. Huawei argues that a final designation would deprive it of liberty interests protected under the Due Process Clause.[186] Consequently, Huawei asserts, the Due Process Clause mandates that Huawei receive four additional procedural protections before any final designation is made: "(1) notice of the evidence against it and the Bureau's reasons for believing that evidence warrants final designation; (2) an opportunity to respond to the evidence, including to cross-examine any witnesses against it; (3) an impartial decisionmaker unaffected by bias, prejudice, or prejudgment; and (4) proceedings free from ex parte contacts."[187]

52. As the Commission expressed in the *Order*, we are skeptical that Huawei is denied a cognizable property or liberty interest protected by the Due Process Clause by designation under section 54.9 of the Commission's rules.[188] Government action implicates Fifth Amendment guarantees of due process only when it deprives an individual of life, liberty, or property.[189] Huawei contends that a final designation would do so in three ways: (1) by injuring its "reputation in connection with the denial of a tangible interest," as framed by the "'stigma-plus' test"; (2) by denying it from pursuing a chosen trade or business; and (3) by debarring it from government programs.[190] In the *Order*, the Commission addressed these issues and found Huawei's arguments unconvincing.[191]

53. Nevertheless, Huawei claims that a final designation would deprive it of a due process interest on these grounds. With respect to the stigma-plus test, Huawei notes that the "Commission itself concedes that 'designation by the Commission as a threat to national security is likely to impose some amount of stigma.'"[192] According to Huawei, a final designation would brand it with a "badge of infamy, and tangibly alter[s] its legal and practical ability to contract with USF recipients."[193] This stigma, Huawei continues, "would also tangibly harm Huawei's business opportunities and goodwill," citing cancellation of equipment orders and contracts.[194] Huawei asserts that "being designated a national security threat . . . will discourage *all* potential customers—whether USF recipients or not—from purchasing and using Huawei equipment."[195]

54. However, Huawei's arguments fail the second prong of the stigma-plus test: a party must show both "(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 law.'"[196] In the *Order*, the Commission assumed, *arguendo*, that the designation would result in some amount of stigma.[197] But demonstrating the existence of stigma alone is not enough. As the Commission explained, while designation may create a "disincentive for carriers to purchase equipment from designated entities," USF recipients can continue purchasing equipment and services

[186] *See* Huawei Comments at 162-67.

[187] Huawei Comments at 168.

[188] *Order*, 34 FCC Rcd at 11460, para. 99.

[189] *Orton Motor, Inc. v. United States Dep't of Health and Human Servs.*, 884 F.3d 1205, 1215 (D.C. Cir. 2018).

[190] Huawei Comments at 163-64.

[191] *Order*, 34 FCC Rcd at 11460-63, paras. 99-103.

[192] Huawei Comments at 165 (quoting *Order*, 34 FCC Rcd at 11461-62 & n.277).

[193] Huawei Comments at 165.

[194] *Id.*

[195] *Id.*

[196] *Order*, 34 FCC Rcd at 11461-62, para. 102 (quoting *Ulrich v. City and County of San Francisco*, 308 F.3d 968, 982 (9th Cir. 2002)).

[197] *Id.* at 11462, para. 102.

from Huawei (albeit without using USF funds).[198] Thus, final designation would not deny Huawei its right to transact with such entities. And Huawei does not identify any other concrete legal right that it has been denied.[199] Huawei does not, for example, cite a protected "business goodwill" interest allegedly impacted by designation,[200] nor the loss of a "cognizable interest in avoiding the loss of government contracting opportunities."[201] Additionally, the fact that USF recipients—let alone carriers not receiving USF support—can continue to contract with Huawei means that a final designation does not reach the level of "broad preclusion" required.[202]

55. Huawei nevertheless maintains that a final designation would "deprive [it] of its liberty to operate its business and pursue its chosen occupation."[203] But while Huawei asserts that it "will lose business,"[204] Huawei has not shown that it will lose the "opportunity to operate [its] business."[205] As explained above, companies are free to transact with Huawei so long as such transactions do not involve the expenditure of USF funds. The loss of some business is not the same as losing the right to operate one's business altogether.

56. Finally, Huawei claims that "final designation would debar Huawei from participating in a government program as a supplier of equipment to USF fund recipients . . . ."[206] By excluding Huawei "from contracting for a 'definite range' of government-funded opportunities," which can occur irrespective "of whether a company directly contracts with the government or serves as a subcontractor," Huawei argues that it is deprived of its liberty interests.[207] But it is unclear how Huawei arrives at this conclusion from the cases it cites. *Kartseva* involved an employee losing her job due to unspecified "counterintelligence concerns" raised by the government, rendering her ineligible to perform the Russian-translation work being performed by her employer.[208] However, at issue was whether the disqualification in *Kartseva* "automatically exclud[ed] [Kartseva] from a definite range of employment opportunities with State or other government agencies" or from working as a Russian translator generally.[209] As the Commission explained in the *Order*, "designation imposes no explicit restriction on designated entities at

---

[198] *Id.* at 11462, para. 103.

[199] *See Gen. Elec. Co.*, 610 F.3d at 310.

[200] *See Marrero v. City of Hialeah*, 625 F.2d 499, 513, 515 (5th Cir. 1980) (state prosecutor's defamatory statements deprived appellants of a Florida-recognized "'legal guarantee of present enjoyment' of goodwill, i.e., the value inhering in the favorable consideration of customers arising from a business' reputation as being well established and well conducted").

[201] *Reeve Aleutian Airways, Inc. v. United States*, 982 F.2d 594, 598 (D.C. Cir. 1993).

[202] *Id.*; *see, e.g.*, *Gen. Elec. Co.*, 610 F.3d 110, 310 (D.C. Cir. 2010) ("the government-imposed stigma [must be] so severe that it 'broadly precludes' plaintiffs from pursuing 'a chosen trade or business'" (quoting *Trifax Corp. v. D.C.*, 314 F.3d 641, 644-45 (D.C. Circ. 2003)); *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 contracting work is 'more than sufficient to preclude a reasonable jury from finding [that the contractor was] broadly precluded from government contracting . . . ." (quoting *Trifax*, F.3d at 644-45)).

[203] Huawei Comments at 166.

[204] Huawei Comments at 166.

[205] Huawei Comments at 163. *See Texas v. Thompson*, 70 F.3d 390, 393 (5th Cir. 1995) (government investigator's claims that a business owner was "a habitual violator who should not be allowed to continue in business," communicated to the business's past and current customers, allegedly caused the business's closure).

[206] Huawei Comments at 166.

[207] *Id.* (citing *Kartseva v. Dep't of State*, 37 F.3d 1524, 1527 (D.C. Cir. 1994)).

[208] *Kartseva*, 37 F.3d at 1526.

[209] *Id.* at 1527.

all," and they remain "free to sell to anyone, including recipients of USF."[210] Huawei thus stretches the meaning of the liberty interest identified in *Kartseva*—the opportunity to obtain a particular kind of employment—to include the opportunity to receive government funding via its transactions with other private entities. Further, *Phillips* involved a state official expressing reservations to potential employers about the fitness of a particular applicant, and his recommendation in that industry may have been tantamount to de facto licensing.[211] The court found "the difference between formal licensing and de facto licensing to be unimportant"[212] and that denying a person credentials that are "practically necessary for pursuing a chosen profession" could represent denial of a liberty interest.[213] Yet, as explained above, Huawei fails to show that prohibiting USF support from being spent on Huawei equipment and services precludes Huawei from pursuing its chosen occupation, let alone that such decision amounts to de facto licensing.

57. Huawei also argues that, liberty interests aside, final designation would deprive it of property interests. Huawei points to "existing contracts with USF recipients and suppliers to USF recipients," which it claims would be interfered with or "effectively abrogate[d] through the designation process . . . ."[214] Yet Huawei ignores that "Commission and judicial precedent make clear that carriers have no vested property interest in ongoing USF support."[215] While USF recipients may be disincentivized from continuing to buy from Huawei, this does not rise to the level of interference or abrogation of a contract. Indeed, Huawei cites no case where a government entity was deemed to have interfered with a contract between two private entities as a result of it withholding funds to one of the parties. And as explained above, designation does not impose any explicit restrictions on their ability to contract with Huawei.

58. *Huawei has been afforded all of the process it was due*. Even if we assume that this final designation implicates Huawei's due process interests, we still find that Huawei has received all protections that the Due Process Clause guarantees here. We find that, contrary to Huawei's argument, the initial designation was adequate to provide Huawei notice that the Commission was considering designating Huawei as a covered company and provided it with ample opportunity to present its case before the Commission prior to adoption of any order with binding legal effect. In fact, the totality of the evidence in this proceeding, including the robust record produced by Huawei in response to the *Notice*, has further indicated that Huawei has been aware of, and had the opportunity to address, on several occasions, concerns regarding its role in the communications supply chain in relation to the since-adopted prohibitive rule.

59. In arguing that it was entitled to cross-examine the analysts and experts that contributed information to secondary sources relied on by the Commission before any final designation, Huawei misunderstands the legal authorities it cites.[216] The cases cited by Huawei stand for the proposition that a person is in some circumstances entitled to cross-examine witnesses that testified in a proceeding concerning that person. Huawei cites no authority for the proposition that an entity has the right to cross-examine individuals who merely contributed to secondary sources produced at different times and for purposes other the proceeding at issue.[217] Because none of the sources here were generated for the

[210] *Order*, 34 FCC Rcd at 11462, para. 103.

[211] *Phillips v. Vandygriff,* 711 F.2d 1217 (5th Cir. 1983), *on reh'g in part*, 724 F.2d 490 (5th Cir. 1984).

[212] *Id.* at 1223.

[213] *Id*.

[214] Huawei Comments at 167.

[215] *Order*, 34 FCC Rcd at 11463, para. 105 & n.288.

[216] *See* Huawei Comments at 170-73.

[217] *See* Huawei Comments at 170 (citing *Greene v. McElroy*, 360 U.S. 474, 466-67 (1959) (concerning right of person whose security clearance was revoked to cross-examine confidential informants)); *Ching v. Mayorkas*, 725 (continued….)

purposes of this proceeding, Huawei does not have a right to cross-examine individuals who merely contributed general information and analysis to these reports.

60. Moreover, due process "is not a technical conception with a fixed content unrelated to time, place and circumstances."[218] Rather, it is "flexible and calls for such procedural protections as the particular situation demands."[219] Here, a consideration of the *Mathews* factors leads to the conclusion that cross-examination was not necessary here. Whatever the weight of Huawei's private rights, the procedure used here afforded Huawei an adequate ability to challenge the conclusions of the materials on which the Commission relied, making the risk of an erroneous deprivation low. Further, the administrative burden of calling the various experts that contributed to the underlying reports would be significant, and do not appear to be justified under the circumstances. In sum, we find that trial-type proceedings were not constitutionally required here, and that the Commission therefore had discretion to choose the form of the proceeding that it would conduct.[220]

61. Huawei further asserts that, because it is entitled to an impartial decisionmaker, any members of the Bureau who "have made public statements demonstrating bias or prejudice toward Huawei or prejudgment of Huawei's status under the USF rule" must be disqualified from participating in the proceeding.[221] Huawei has not, however, identified any public statements by Bureau staff relating to this proceeding or other indications of bias or prejudgment by Bureau staff.

62. Finally, contrary to Huawei's argument, there were no improper *ex parte* contacts in this designation proceeding.[222] Huawei overlooks that this proceeding began as a rulemaking that resulted in the adoption of a final rule.[223] Based on the record developed in the rulemaking, the Commission decided to adopt rules governing adjudications and commenced these adjudicatory designation processes.[224] The *ex parte* contacts Huawei identifies occurred *before* its designation proceeding began, *i.e.*, before the initial designation order was issued.[225] At that time, no adjudication had yet commenced., and the proceeding could only be considered a rulemaking. As Huawei acknowledges, rulemakings are classified under the Commission's rules as "permit-but-disclose" proceedings.[226] In such proceedings, *ex parte*

(Continued from previous page)
F.3d 1149, 1158 (9th Cir. 2013) (concerning right of petitioner for visa to cross-examine prior spouse); *Bus Commc'ns, Inc. v. U.S. Dep't of Educ.*, 739 F.3d 374, 380 (8th Cir. 2013) (concerning right of company to cross-examine individuals providing information for agency report); *Cooper v. Salazar*, 196 F.3d 809, 815 (7th Cir. 1999) (evaluating constitutionality of procedures used for investigating and resolving discrimination claims).

[218] *Mathews v. Eldridge*, 424 U.S. 319, 334, 96 S.Ct. 893, 47 L.Ed.2d 18 (1976) (internal quotation marks omitted).

[219] *Id.*

[220] *See Vt. Yankee Nuclear Power Corp. v. Nat. Res. Def. Council, Inc.,* 435 U.S. 519, 543-44 (S. Ct. 1978).

[221] Huawei Comments at 173. In response to Huawei's argument about the Appointments Clause of the Constitution, *see* Huawei Comments at 125 n.23, we note that the Bureau acts on delegated authority for the full Commission. *See* 47 CFR § 0.191.

[222] *See* Huawei Comments at 174-76.

[223] *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 (2018) (seeking comment on proposed rule); *see Order*, para. 2 (adopting "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").

[224] *See Qwest Servs. 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).

[225] *See* Huawei Comments at 23-24. Although some parties have submitted filings labeled as *ex parte* in the Huawei designation docket, these all concerned the rulemaking only and not Huawei's designation specifically.

[226] *See* 47 CFR § 1.1206(a)(1) (classifying informal rulemakings as "permit but disclose" proceedings); Huawei Comments at 174.

presentations are permitted as long as certain disclosure requirements are followed.[227] Huawei does not identify any failure of compliance with these requirements, and, even if there were any such failure, those *ex parte* contacts occurred before Huawei's designation proceeding began. Consequently, Huawei is incorrect to the extent it asserts that there have been unlawful ex parte contacts in its designation proceeding.[228]

D. Effective Date

63. The final designation of Huawei is effective immediately upon release of this Order. We conclude that the risks to our national communications networks and communications supply chain posed by Huawei's equipment necessitate immediate implementation of our designation.[229] This conclusion is consistent with the Commission's finding of good cause to expedite implementation of the rules adopted in the *Protecting Against National Security Threats Order* and make them effective upon publication in the Federal Register.

64. We decline the Rural Wireless Association's request to further delay any final determination of Huawei until such time as a reimbursement mechanism is established.[230] Nothing in the Commission's rule or the Secure Networks Act requires the Commission to continue funding equipment and services posing a national security threat to communications networks or the communications supply chain until a reimbursement mechanism is established. On the contrary, the Secure Networks Act directs the Commission to prohibit the use of USF funds for covered equipment and services within 180 days after its enactment, while providing the Commission one year to complete the rulemaking to establish the reimbursement program.[231] Additionally, this designation does not require any USF recipient to remove and replace existing equipment. Rather, the effect of this designation is merely to prohibit the future use of USF support to purchase, obtain, maintain, improve, modify, or otherwise support any such equipment or services. Although we recognize that prohibiting the use of USF funds for Huawei equipment or services may burden USF recipients who use such equipment or services, as the Commission explained in the *Order*, that burden pales in comparison to the cost of delaying implementation of this designation and allowing USF funds to fund equipment and services that threaten our national security.[232] We therefore see no reason to delay the designation.

---

[227] *See* 47 CFR § 1.1206(a).

[228] Even if this proceeding is classified as a restricted proceeding, the only *ex parte* contacts identified by Huawei took place before the initial designation, which had no binding legal effect. *See* Huawei Comments at 23-24. The filings on the Commission's docket do not indicate that Huawei was discussed in any ex parte meeting that took place during the period that the Bureau was deliberating whether to make a final designation of Huawei as a covered company.

[229] *Order*, 34 FCC Rcd at 11483, paras. 168-69. As explained in the *Order*, the prohibition of the use of USF funds to procure Huawei equipment or services will apply to the E-Rate and Rural Health Care programs for funding year 2020. *See Order*, 34 FCC Rcd at 11456-57, para. 86.

[230] *See* RWA Comments at 1; RWA Secure Networks Act PN Comments at 3; RWA NTIA Filing Comments at 3.

[231] *Compare* Secure Networks Act § 3(b) *with* Secure Networks Act § 4(g)(2).

[232] *Order*, 34 FCC Rcd at 11452-53, para. 75. Providers may, of course, seek a waiver of this prohibition if necessary. *Id.*

IV. ORDERING CLAUSE

65. Accordingly, IT IS ORDERED, pursuant to sections 1-4, 201(b), 229 and 254 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151-154, 201(b), 229, 254, and section 54.9(b) of the Commission's rules, 47 CFR § 54.9(b), that this Order IS ADOPTED and EFFECTIVE IMMEDIATELY UPON RELEASE. This action is taken under delegated authority pursuant to Sections 0.191 and 0.392 of the Commission's rules, 47 CFR §§ 0.191 and 0.392.

FEDERAL COMMUNICATIONS COMMISSION

Lisa Fowlkes
Chief
Public Safety and Homeland Security Bureau