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

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

MEMORANDUM OPINION AND ORDER

Adopted: December 10, 2020 **Released: December 11, 2020**

By the Commission: Chairman Pai and Commissioner Carr issuing separate statements.

I. INTRODUCTION

1. Broadband networks play an ever-increasing role in our economy, connecting Americans to their doctors, teachers, coworkers, friends, and family, and supporting critical infrastructure like power grids, transportation networks, financial markets, and emergency communications. The need to protect communications networks from external threats grows in lockstep with the growing role these networks play in Americans' lives. Last year, we acted to protect America's communications networks and the communications supply chain by adopting a rule prohibiting the use of universal service support to purchase or maintain equipment and services from companies posing a national security threat to the integrity of communications networks or the communications supply chain.[1] In the *Protecting Against National Security Threats Order*, we initially designated Huawei Technologies Co., along with its parents, affiliates, and subsidiaries, as a covered company based on the substantial body of evidence demonstrating the risks posed by Huawei to the security of U.S. communications networks and directed the Public Safety and Homeland Security Bureau (Bureau) to determine whether to issue a final designation of Huawei as a covered company.[2]

2. On June 30, 2020, based on the totality of evidence before it, the Bureau issued a final designation of Huawei as a covered company. As a result, funds from the Commission's Universal Service Fund (USF or Fund) may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by Huawei.[3]

3. Huawei sought review of the Bureau's final designation. Because we can—and must—take action to protect the security of U.S. communications networks, and because we conclude the Bureau acted appropriately, we deny Huawei's Application for Review of the *Final Designation Order*.[4] In so

[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*).

[2] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11439-40, 11449, paras. 43, 64.

[3] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Final Designation Order*); *see also* 47 CFR § 54.9(a).

[4] Application for Review of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., PS Docket No. 19-351 (filed Jul. 30, 2020) (Huawei AFR); *Final Designation Order*.

doing, we affirm the Bureau's determination that Huawei poses a threat to the security and integrity of our nation's communications networks or the communications supply chain.

II. BACKGROUND

A. The Bureau's Designation of Huawei

4. Among the Commission's core responsibilities, Congress has charged the Commission with protecting the nation's communications networks "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. . . ."[5] The Commission has therefore taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats. In particular, in November 2019, we adopted the *Protecting Against National Security Threats 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.[6]

5. In adopting the rule, the Commission determined that it had independent legal authority to prohibit Universal Service Fund recipients from spending public monies from the Fund on covered equipment and services. First, the Commission adopted this rule as an exercise of its authority under section 254 of the Act to place conditions on the use of universal service support to serve the statutory purpose of promoting the availability of quality telecommunication equipment and services, and because it is critical to the provision of "quality services"[7] that support from the Fund be spent on secure networks and not on equipment and services from companies that threaten national security.[8] Second, the Commission relied on its section 201(b) authority to promulgate rules necessary in the public interest to carry out the provisions of the Act.[9] Finally, the Commission determined that promulgating this rule implemented section 105 of the Communications Assistance for Law Enforcement Act (CALEA).[10]

6. The Commission's initial designation of Huawei as a covered company for purposes of our rules followed an extensive examination of the record developed in that proceeding.[11] The Commission found that Huawei posed "a unique threat" to the security and integrity of the nation's communications networks and communications supply chain because of its size, close ties to the Chinese government, and security flaws identified in its equipment.[12] The Commission noted that Huawei's ties to the Chinese government and military 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 propensity for intervening in the affairs of Chinese companies make it susceptible to Chinese governmental pressure to participate in espionage activities.[13] The Commission also relied on reports highlighting known vulnerabilities in Huawei equipment, which led other countries to bar the use of such equipment.[14] Furthermore, the Commission was informed by the steps taken by Congress and the

[5] 47 U.S.C. § 151.

[6] 47 CFR § 54.9(a); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, para. 26.

[7] 47 U.S.C. § 254(b)(1).

[8] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11434, para. 29.

[9] 47 U.S.C. § 201(b); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11436, para. 34.

[10] 47 U.S.C. § 1004; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11436, para. 35.

[11] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11439-40, para. 43.

[12] *Id*. at 11439-41, paras. 43-46.

[13] *See id*. at 11442, para. 48.

[14] *See id*. at 11444-47, paras. 53-57.

Executive Branch to restrict the purchase and use of Huawei equipment, including the decision by the Department of Defense to remove Huawei devices from sale at U.S. military bases and from its stores worldwide.[15] In addition, the Commission observed that Huawei's founder, Ren Zhengfei, had previously served as a director in the People's Liberation Army of China and China's 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 People's Liberation Army.[16] The Commission further explained that Huawei has been "reported to receive vast subsidies from the Chinese government."[17]

7. After the initial designation of Huawei, the Commission directed the Bureau to implement the next steps in the designation process. Following publication of the initial designation in the *Federal Register*, the Bureau issued a Public Notice on January 3, 2020, seeking comment on the designation.[18]

8. On June 9, 2020, the National Telecommunications and Information Administration (NTIA) submitted a filing in this proceeding, "as the President's principal adviser on telecommunications and information policy, and on behalf of the Executive Branch," explaining that the Executive Branch "fully supports" the designation of Huawei and providing the Executive Branch's analysis of matters including the legal framework in China, the national security risks posed specifically by Huawei, and the national security interests demonstrated by its violations of U.S. law.[19] The Bureau provided an opportunity for Huawei and other interested parties to respond to NTIA's filing in a Public Notice issued June 9, 2020.[20] Four parties, including Huawei, filed comments in response to NTIA's filing.[21]

9. In the *Final Designation Order*, released on June 30, 2020, the Bureau found a substantial body of evidence in the record about the continuing risks from Huawei and its 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.[22] The Bureau further determined that the authoritarian

[15] *See id*. at 11442, 11444, paras. 48, 52.

[16] *See id*. at 11443, para. 50.

[17] *Id*. at 11443-44, para. 51.

[18] *Public Safety and Homeland Security Bureau Announces Comment Date on the Initial Designation of Huawei Technologies Company as a Covered Company in the National Security Supply Chain Proceeding*, PS Docket No. 19-351, Public Notice, 35 FCC Rcd 196 (PSHSB Jan. 3, 2020).

[19] *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 and 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*, IB Docket No. 97-142, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919, para. 63 (1997); *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3362-63, para. 2 (2019).

[20] *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 and 19-352, 35 FCC Rcd 5791 (PSHSB Jun. 9, 2020).

[21] *See generally* Huawei Comments (filed June 19, 2020) (Huawei NTIA Filing Comments); NTCA—The Rural Broadband Association Comments (filed June 19, 2020) (NTCA NTIA Filing Comments); USTelecom Comments (filed June 19, 2020) (USTelecom NTIA Filing Comments).

[22] *Final Designation Order*, 35 FCC Rcd at 6605-606, para. 4.

nature of the Chinese government provides little legal or political recourse, even if Huawei wished to resist legal pressure from the Chinese government.[23] Finally, the Bureau determined that there has been a demonstrated pattern of security flaws found in Huawei equipment.[24] The Bureau determined that these facts have led the U.S., as well as its allies, to significantly restrict the purchase and integration of Huawei equipment and services into communications infrastructure.[25] The Bureau accordingly determined that Huawei poses a threat to the nation's communications networks and the communications supply chain.

B. Huawei's Application for Review

10. On July 30, 2020, Huawei filed an Application for Review challenging the *Final Designation Order* pursuant to section 1.115 of the Commission's rules.[26] Specifically, Huawei argues that the Commission lacked authority to adopt the rule pursuant to which Huawei was designated as a national security threat.[27] Huawei further argues that the Bureau violated the Administrative Procedure Act by: (1) relying on unsupported evidence to issue the designation;[28] (2) singling out Huawei for a designation when other similarly situated identified entities have not been designated as national security threats;[29] (3) failing to consider Huawei's counterevidence that it is not an instrument of the Chinese government, military, or Chinese intelligence, but an autonomous private entity;[30] and (4) failing to follow Commission precedent.[31] Additionally, Huawei argues that the *Final Designation Order* was unconstitutional because: (1) the decision to designate Huawei was issued due to congressional pressure;[32] (2) Commissioners' statements demonstrated prejudice;[33] and (3) Huawei's constitutionally protected due process rights have been violated.[34]

III. DISCUSSION

11. We affirm the Bureau's decision to finally designate Huawei, as well as its parents, affiliates, and subsidiaries, as companies posing a national security threat to the integrity of our nation's communications networks and the communications supply chain. Based on the record before us, we conclude, as the Bureau did, that Huawei is highly susceptible to Chinese government coercion, its equipment has known security risks and vulnerabilities, and we have sufficient legal authority to make such a final designation.

[23] *Id*. at 6615-16, paras. 24-25.

[24] *Id*. at 6605-606, para. 4.

[25] *See id*. at 6616, para. 28. Such concerns have been further buttressed by Sweden's recent decision to disallow Huawei equipment in its networks, after Sweden's security services called China "one of the biggest threats against Sweden." *See* CNBC, *Sweden bans Huawei, ZTE from upcoming 5G networks* (Oct. 20, 2020), https://www.cnbc.com/2020/10/20/sweden-bans-huawei-zte-gear-from-5g-spectrum-auction.html.

[26] *See* Huawei AFR.

[27] *Id*. at i, 2-3, 9-10.

[28] *Id*. at i, 1-2, 4, 9-10.

[29] *Id.* at 18.

[30] *Id*. at i, 2, 17-18.

[31] *See id*.

[32] *Id*. at i, 2, 19-21.

[33] *Id*. at 21.

[34] *Id*. at 21-25.

A. The Bureau's Decision to Finally Designate Huawei as a National Security Threat Was Proper

12. First, we find that the *Final Designation Order* was based on the totality of the record,[35] relying on extensive evidence about the risks Huawei poses to the nation's communications networks.[36] In its decision, the Bureau carefully examined the record, including determinations by Congress, the President, other executive agencies, experts on Chinese law and government, U.S. and allied intelligence services, and security experts to assess the risks posed by Huawei. The Bureau's conclusion rested on its "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."[37] We agree that the record in this case compels the Bureau's conclusions in its *Final Designation Order*.

13. In reaching its conclusion, the Bureau determined that Huawei, as an entity subject to Chinese governance, is subject to Chinese laws requiring it to facilitate espionage on behalf of the Chinese intelligence apparatus.[38] The facts presented, taken in light of the totality of the evidence, paint a picture of a company that, either willingly or through compulsion, has and will continue to support the espionage and surveillance activities of the Chinese government.[39] As such, we agree with the Bureau that Huawei poses a sufficient threat to communications networks and the communications supply chain as to warrant prohibiting recipients of public funds from the Universal Service Fund from using such funds for Huawei services and equipment. Nothing in Huawei's Application for Review, relying as it does on its purported "independence" from the Chinese government, allays these concerns. We therefore uphold the Bureau's *Final Designation Order*.

14. We disagree with Huawei's argument that the Bureau violated the Administrative Procedure Act by failing to support the *Final Designation Order* with reliable and probative evidence in the record.[40] As outlined below, and in the *Final Designation Order*, experts from Executive Branch agencies, U.S. and allied intelligence agencies, and outside experts have all concluded that Huawei poses a threat to the security of U.S. communications networks and the communications supply chain. We find the evidence cited by the Bureau to be both reliable and probative.

1. Huawei is susceptible to Chinese government coercion.

15. Specifically, we agree that Huawei is susceptible to legal and extralegal coercion and poses risks to the security of our nation's communications networks.[41] We find that Huawei's close ties

[35] *Final Designation Order*, 35 FCC Rcd at 6608, para. 10.

[36] *See Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, para. 44. Both the Commission in its *Protecting Against National Security Threats Order* and the Bureau in its *Final Designation Order* "compiled and reviewed additional classified national security information that provides further support for [its] determinations." *Id.* at 11440, n.124; *see also Final Designation Order*, 35 FCC Rcd at 6608, n.35. The Commission continues to find that the "publicly available information in the record [is] sufficient to support these designations," and that the "compiled and reviewed additional classified national security information . . . provides further support for [its] determinations." *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, n.124; *see also* 47 CFR § 54.9(a). This information was contained in classified Appendix E to the *Protecting Against National Security Threats Order*.

[37] *Final Designation Order*, 35 FCC Rcd at 6609, para. 12.

[38] *Id*. at 6605-606, 6608-609, 6613-14, 6616, paras. 4, 11, 21-22 and 27.

[39] *Id*. at 6608, para. 10.

[40] Huawei AFR at i, 1-2, 4, 9-10.

[41] *See Final Designation Order*, 35 FCC Rcd at 6609-10, 6611, 6615-16, paras. 14, 17, 24-25; *see also* NTIA Letter at 8 ("As long as Huawei . . . [is] subject to the legal and extralegal influence and control of the Chinese government and the [Chinese Communist Party], there are doubts that the compan[y] can be trusted to comply fully with U.S.

(continued….)

to the Chinese government, both at the level of ownership and at the employee level, along with its legal obligations to assist the Chinese government, present far too great a risk to U.S. national security to continue to subsidize the use of Huawei equipment and services with taxpayer money.

16. We first conclude that China's National Intelligence Law grants the Chinese government the power to compel Huawei to assist it in espionage activities.[42] Article 7 of the National Intelligence Law states, "[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets that they are aware of."[43] Article 14 moreover provides that the Chinese intelligence apparatus "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[44] Further, Article 16 expressly allows Chinese intelligence services to enter companies' restricted areas and collect files at will.[45] And Article 17 goes still further, providing that intelligence services may "have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings; and when necessary, they may set up relevant work sites, equipment, and facilities."[46]

17. We also find that the National Intelligence Law appears to provide no flexibility for companies or individuals to refuse or appeal these requests from the Chinese government. The Bureau, in its *Final Designation Order*, properly relied on legal interpretations from the Executive Branch, which determined that Chinese law imposes "affirmative legal responsibilities on [People's Republic of China] 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."[47] Outside legal experts have likewise argued 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.'"[48] We agree with the Bureau's reliance on the analysis by the Executive Branch of the U.S. government,[49] and particularly the Executive Branch's explanation of how companies such as Huawei are beholden to the legal and extralegal controls of the Chinese government and Chinese Communist Party.[50] As a result, we conclude,

(Continued from previous page)
law . . . . Huawei has allegedly offered bonuses to its employees based on the value of information they stole from other globally-situated companies.").

[42] *Final Designation Order*, 35 FCC Rcd at 6613-14, para. 22 (citing NTIA Letter at 5).

[43] NTIA Letter at 5; *see also Final Designation Order*, 35 FCC Rcd at 6613-14, para. 22. This and subsequent quotations from the National Intelligence Law are taken from China Law Translate, *National Intelligence Law of the P.R.C.* (June 2017), *available at* https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/, which NTIA used in its letter.

[44] NTIA Letter at 5; *see also Final Designation Order*, 35 FCC Rcd at 6613-14, para. 22 (citing Chinese National Intelligence Law, Articles 14 and 17); 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).

[45] NTIA Letter at 5.

[46] *Id*.

[47] *Final Designation Order*, 35 FCC Rcd at 6615-16, para. 25 (citing NTIA Letter at 5).

[48] *Id*. (citing 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) (internal punctuation omitted)).

[49] NTIA Letter at 1.

[50] *Final Designation Order*, 35 FCC Rcd at 6607, n.29 (citing NTIA Letter at 4-8). The Commission has historically found it appropriate to seek and accord deference to the expressed views of the Executive Branch in (continued….)

based on our analysis of the record, that Huawei is susceptible to both legal and political coercion by the Chinese government, and that susceptibility presents profound risks to the security of our nation's communications networks.

18. For its part, Huawei asserts, and the Commission already addressed in the *Protecting Against National Security Threats Order*,[51] that the Commission's interpretation of the National Intelligence Law was based on a "misunderstanding" because, according to Huawei, the Commission's interpretation of specific National Intelligence Law articles does not: (1) empower the Chinese government to access Huawei's internal communications systems or plant spyware; (2) empower the Chinese government to interfere in the operations of privately-owned companies like Huawei; (3) apply to Huawei subsidiaries in the United States; and (4) apply because the articles described are purely defensive.[52] However, NTIA expressed the Executive Branch's full support of our initial designation of Huawei as a security threat and provided the Executive Branch's legal conclusion that China's National Intelligence Law and Cybersecurity Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for the government's intelligence gathering activities.[53] We are not persuaded by Huawei's argument in light of the Executive Branch's interpretation of the National Intelligence Law,[54] a fact that Huawei concedes by omission in its Application for Review. We, like the Bureau, give greater weight to the Executive Branch's interpretation of the National Intelligence Law, rather than Huawei's self-serving interpretation.[55]

19. Huawei's argument that "[b]y expressly making its designation of Huawei turn on an interpretation of foreign law, the Bureau left open the possibility that its construction of foreign law could be reversed on judicial review" is unavailing.[56] We acknowledge that Huawei and the Executive Branch have different interpretations of Chinese law, but consistent with Commission precedent, we accord deference to NTIA's risk-based interpretation of Chinese intelligence law.[57] Moreover, even if we were to set aside the issue of interpretation of Chinese law, the other evidence in the record is more than sufficient to conclude that Huawei poses an unacceptable risk to the security of our nation's communications networks and to the communications supply chain.

20. We likewise reject Huawei's claim that the National Intelligence Law does not apply to Huawei's U.S. subsidiary because the National Intelligence Law is only applied for "purely defensive" reasons, Chinese law does not have extraterritorial effect, and Huawei has never been asked by Chinese governmental entities to conduct espionage on behalf of the Chinese government.[58] We reject that argument after considering the broad sweep of Article 11 of the National Intelligence Law, which authorizes Chinese intelligence agencies to act abroad, and the Executive Branch's interpretation of the Chinese legal regime, which holds that Chinese law imposes affirmative legal responsibilities on both

(Continued from previous page)
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*, IB Docket No. 97-142, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23919, para. 63 (1997); *China Mobile International (USA) Inc.*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3362-63, para. 2 (2019).

[51] *See Final Designation Order*, 35 FCC Rcd at 6613, para. 21.

[52] Huawei AFR at 14-15.

[53] NTIA Letter at 5.

[54] *See Final Designation Order*, 35 FCC Rcd at 6615-16, paras. 24 and 26 & n.87-88.

[55] *See id*. at 6616, para. 26.

[56] *Iracheta v. Holder*, 730 F.3d 419, 423 (5th Cir. 2013); *see* Huawei AFR at 11, 13.

[57] *See Final Designation Order*, 35 FCC Rcd at 6607, para. 8.

[58] Huawei AFR at 15.

Chinese and foreign citizens, companies, and organizations operating in China to assist with Chinese intelligence-gathering activities.[59] We agree with the Bureau's determination that, "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."[60]

21. Similarly, we find that Huawei USA employees are vulnerable to demands from Huawei China, despite Huawei's unsubstantiated claims to the contrary. By way of example, last year a Grand Jury returned an indictment against Huawei Device Co. LTD. and Huawei Device USA, Inc. alleging the companies knowingly stole a trade secret from T-Mobile,[61] and that Huawei USA engineers were pressured by Huawei China engineers to provide them with the technical specifications for certain T-Mobile technology in violation of T-Mobile's non-disclosure agreement. Indeed, when the Huawei USA engineers initially refused to share the information with Huawei China engineers, Huawei China pressured the Huawei USA employees for months until they provided photos and other details of T-Mobile's proprietary design. After continued pressure by email, and not having the specifications Huawei China required, the Chinese engineers sent employees from China to Seattle to intimidate and coerce the Huawei USA employees directly. During that trip, using Huawei USA employees access badges, Huawei China employees gained unauthorized access to T-Mobile's laboratory and photographed confidential T-Mobile documents.[62] This is but one example of the myriad ways Huawei coerces its employees to assist in reconnaissance activities. We therefore find that employees of Huawei's U.S. subsidiaries are susceptible to coercion by Huawei China, and by extension Chinese intelligence, and universal service support should not be used to fund such equipment given Huawei's demonstrated history of cooperating with Chinese government espionage activities.

22. While Huawei disagrees with the Commission's interpretation of the National Intelligence Law,[63] Huawei's more generous interpretation of the law does not mitigate our concerns in light of the authoritarian nature of the Chinese government and the lack of judicial independence of the Chinese court system, which can support the Chinese government in compelling Huawei to comply regardless of whether the law specifically directs it. We agree with the Bureau that "state actors, . . . notably China, . . . have supported extensive and damaging cyberespionage efforts in the United States,"[64] and there exists a "substantial body of evidence" about the risks of certain equipment providers like Huawei.[65] Indeed, U.S. allies have discovered multiple instances in which the Chinese government has,

[59] *See Final Designation Order*, 35 FCC Rcd at 6614, para. 23; *see also* NTIA Letter at 5.

[60] *Final Designation Order*, 35 FCC Rcd at 6620-21, para. 38 (citing *Protecting Against National Security Threats Order*, 34 FCC Rcd at 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")).

[61] *See USA v. Huawei Device Co. Ltd, et al*., No. CR-19-010 (U.S.D.C. W.D. Wash. 2019).

[62] *See id*., paras. 14-26, 27-30.

[63] Huawei AFR at 14-15.

[64] *Final Designation Order*, 35 FCC Rcd at 6609, para. 14 (quoting Telecommunications Industry Association Comments, WC Docket No. 18-89, at 10 (rec. June 1, 2018)).

[65] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, para. 44 (quoting USTelecom Comments, WC Docket No. 18-89, at 3 (rec. June 1, 2018) ("[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. . . .")); *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); *Protecting Against National Security Threats 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) (discussing

(continued….)

through its Ministry of State Security, targeted intellectual property and other sensitive commercial information in Europe, Asia, and the United States.[66] And the Bureau was correct to give weight to retired United States Army Lieutenant General and former U.S. National Security Advisor H.R. McMaster's observation that "the integrated nature of the Chinese Communist Party's military and economic strategies is what makes it particularly dangerous to the United States and other free and open societies."[67] As Lieutenant General McMaster wrote, "[i]n 2014 and then again in 2017, the party declared that all Chinese companies must collaborate in gathering intelligence,"[68] and "Chinese companies work alongside universities and research arms of the People's Liberation Army,"[69] and "Chinese cybertheft is responsible for what General Keith Alexander, the former director of the National Security Agency, described as the 'greatest transfer of wealth in history.'"[70] Indeed, Lieutenant General McMaster explained that "Chinese espionage is successful in part because the party is able to induce cooperation, wittingly or unwittingly, from individuals, companies, and political leaders."[71]

23. Next, we find that the Chinese government appears to have the means to tamper with Huawei's products in aid of its espionage activities.[72] The record in this proceeding suggests that Chinese intelligence agencies have the ability to tamper with Huawei's products in both the design and manufacturing processes.[73] Moreover, the Executive Branch's legal conclusion that China's National Intelligence Law and Cybersecurity Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for the government's intelligence gathering activities is consistent with that determination.[74] Given the Executive Branch's expertise in both foreign affairs and national security, we give significant weight to NTIA's conclusions and find that the Bureau properly relied on these conclusions, among other ample record evidence, to determine that Huawei poses a national security threat to communications networks and the communications supply chain.[75]

24. The Bureau's finding that Huawei is subject to influence by the Chinese government is buttressed by NTIA's analysis that the need to maintain "a good relationship with the [Chinese Communist Party] is a prerequisite for business success [and] has led companies like Huawei to be active

(Continued from previous page)
China's "notorious reputation for persistent industrial espionage" and its use of close collaboration between government and industry).

[66] *Final Designation Order*, 35 FCC Rcd at 6609-10, para. 14; *see* RWR 2019 Report at 8; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, para. 44.

[67] *Final Designation Order*, 35 FCC Rcd at 6612, para. 19 (quoting H.R. McMaster, What China Wants, *The Atlantic*, May 2020 at 70, 71, 73).

[68] H.R. McMaster, What China Wants, *The Atlantic*, May 2020.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Final Designation Order*, 35 FCC Rcd at 6610, para 15.

[73] *Id*. at 6620, 6627, paras. 36 and 51; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440-41, para. 45; Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE at 3 (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (*HPSCI Report*) (observing that during product development, "malicious hardware or software [could be] implant[ed] into critical telecommunications components and systems").

[74] NTIA Letter at 5.

[75] *Final Designation Order*, 35 FCC Rcd at 6607, 6615, n.29 & n.88.

participants in achieving the goals of the State."[76] We agree that this factor further supports the conclusion that Huawei is highly subject to coercive pressure from the Chinese government.[77] Even if we accept Huawei's claims that it would resist Chinese legal pressure to assist in espionage, the fact remains that Huawei must maintain its working relationship with the Chinese Communist Party, and the risk is far too great that Huawei will choose its business success over protecting the security of U.S. communications networks.

25. Moreover, we are skeptical that Huawei can actually obtain legal relief from the Chinese court system if it attempted to resist pressure to assist in espionage, given Chinese courts' lack of independence from the Chinese authoritarian governmental system. 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.[78] As NTIA points out, "one of the conditions for becoming a judge is 'supporting . . . the leadership of the Communist Party of China and the socialist system.'"[79] Indeed, as the Bureau noted, 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.'"[80] We agree with the Bureau that Huawei may not even be inclined to seek such judicial relief, given the evidence that it has in fact assisted other foreign governments in spying on political opponents.[81] Huawei claims that the Chinese government prioritizes economic growth over espionage, but whatever priorities the Chinese government chooses to emphasize at any particular point in time, the Bureau was accurate about the incentive and ability of that government to use its influence over private companies, and recent developments vindicate the Bureau's skepticism.[82]

26. We also disagree with Huawei's contention that the Bureau failed to rebut Huawei's claims that it is a private company not subject to Chinese government coercion.[83] It claims that the Bureau ignored evidence purporting to show it is not controlled or influenced by the Chinese government

[76] 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.*

[77] *See id*. at 8 ("As long as Huawei . . . [is] subject to the legal and extralegal influence and control of the Chinese government and the [Chinese Communist Party], there are doubts that the compan[y] 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.").

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

[79] *Id*. 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.*

[80] *Final Designation Order*, 35 FCC Rcd at 6616, para. 26 (citing RWR 2019 Report at 21-22 (quoting Qiang)).

[81] 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.

[82] *See* Chris Buckley and Keith Bradsher, *China's Communists to Private Business: You Heed Us, We'll Help You*, New York Times (Sept. 17, 2020), https://www.nytimes.com/2020/09/17/business/china-communist-private-business.html (reporting that "Xi Jinping, China's current leader, has his own message for the country's private businesses that reflects a drive for both economic growth and greater Communist Party control: We're here to help you, but you must also help and heed us. The party that leads the world's second-largest economy after the United States laid the groundwork this week for greater party influence over private business . . . .").

[83] Huawei AFR at 10-11, 15-16.

and that the assessment of evidence that the Bureau based its designation upon is unreliable.[84] While Huawei contends that it is independent of Chinese government control and that it does not receive special treatment from the government,[85] the Bureau was correct to give little weight to this argument, and we instead more heavily weigh the Executive Branch's expert national security judgment that Huawei has in fact benefited from Chinese government largesse and is treated as a state-owned enterprise and national champion.[86] Huawei seems to agree that the Bureau was appropriate to give more weight to the Executive Branch's interpretation. It argues that national security assessments should be "exclusively" assigned to Congress, the Department of Commerce, and Executive Branch agencies with national security expertise.[87] This is precisely what we and the Bureau have done here—looked for guidance from Congress and agencies with expertise in national security issues in reaching our designation determination.[88] Moreover, Huawei appears to assume that the Bureau had to show that Huawei received government support on more favorable terms than it would have received from private sources.[89] But Huawei offers no support for its argument, and indeed, the fact that it receives such backing from the Chinese government is itself reason to doubt Huawei's claims of independence.

27. We similarly conclude that Huawei's demonstrably close ties to the Chinese military support this designation. Among Huawei employees in the union that purportedly controls 99% of shares in Huawei, 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 counterintelligence, foreign intelligence, and political security activities.[90] Moreover, in June 2020, the United States Department of Defense released a list of 31 companies operating directly or indirectly in the United States with ties to the Chinese military, including Huawei.[91] Huawei concedes that its founder Ren Zhengfei previously served as a Deputy Director in the Civilian Engineering Corps of the People's Liberation Army.[92] In addition to his one percent ownership of shares, Huawei acknowledges that its charter provides Ren with certain unusual

[84] *Id*. at 3.

[85] *Final Designation Order*, 35 FCC Rcd at 6612, n.63 (citing 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).

[86] *Final Designation Order*, 35 FCC Rcd at 6611, para. 17.

[87] *See* Huawei Comments at 57-77 (filed Feb. 3, 2020) (Huawei Designation Comments); *see, e.g.*, *Holy Land Found. for Relief & Devel. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003) (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 v. U.S. Dep't of State*, 182 F.3d 17, 19 (D.C. Cir. 1999).

[88] *See id*.

[89] Huawei AFR at 12-13.

[90] Christopher Balding, Huawei Technologies' Links to Chinese State Security 1 (July 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 (July 8, 2019), https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7.

[91] *See* Press Release, Department of Defense, DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA, (Aug. 28, 2020), https://www.defense.gov/Newsroom/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/source/email/.

[92] Huawei Designation Comments at 133.

veto powers, "including the right to veto amendments to governance documents[93] or to veto increases or decreases in the registered capital of Huawei."[94] Huawei relies on the fact that Ren has not used his veto, but does not explain why that should allay our concerns about Huawei's connections to the Chinese government and military.[95] The Bureau was also correct to rely on the fact that Huawei has an internal Communist Party organization, which NTIA explains gives the Chinese government influence over all levels of decision making within Huawei.[96] Huawei argues that Communist Party cells have less influence in private companies than state-owned enterprises, but that hardly quells concerns about the Party's influence on Huawei.[97]

28. We also conclude that the Chinese government has both the intent and means to use Huawei's resources for espionage purposes.[98] It is evident, therefore, that Universal Service Fund support should not be used in a manner that undermines the security of our network and assists the Chinese government in conducting espionage. As the U.S. Attorney General argued in the proceeding leading to our adoption of the rule barring universal service support to companies that pose a threat to security of communications networks, "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.[99] The totality of the evidence in this case weigh heavily against providing U.S. public funding for a company that has both a history of and a legal obligation to assist a foreign adversary in committing acts of espionage against the United States.

2. Huawei's equipment presents significant security vulnerabilities.

29. We also conclude that the security risk to our communications networks from permitting universal service support to be used for the purchase of Huawei equipment is significant given vulnerabilities in that equipment.[100] In particular, the Bureau relied on the United Kingdom's Huawei Cyber Security Evaluation Centre Oversight Board, which found significant defects in Huawei's software engineering and cyber security processes. The Cyber Security Evaluation Centre Oversight Board judged that that these defects in Huawei's processes created significant risks to communications networks in the United Kingdom.[101] As a result of the its conclusions, the United Kingdom recently banned Huawei from the core of its communications networks and from building a 5G network in the country, and the Bureau credited these conclusions in finding that Huawei posed a national security threat to U.S. networks given

[93] We also disagree with Huawei's argument that the Bureau relied "largely on absence of evidence" about Huawei's ownership and corporate governance. Huawei AFR at 5.

[94] Huawei Designation Comments at 133.

[95] Huawei AFR at 6-7. In other contexts, the Commission has consistently found that veto rights that extend beyond well recognized protections against dilution of investors' interests may be sufficient to confer *de facto* control on the holder of those veto rights. *See, e.g., SNR Wireless LicenseCo, LLC v. FCC*, 868 F.3d 1021 (D.C. Cir. 2017) (investor "required [licensees] to consult it on every important aspect of their business plans").

[96] *Final Designation Order*, 35 FCC Rcd at 6612-13, para. 20; NTIA Letter at 6-7.

[97] And new guidelines "imply[] that internal Communist Party committees will be more active in companies." Chris Buckley and Keith Bradsher, *China's Communists to Private Business: You Heed Us, We'll Help You*, New York Times (Sept. 17, 2020), https://www.nytimes.com/2020/09/17/business/china-communist-private-business.html.

[98] *See Final Designation Order*, 35 FCC Rcd at 6605-606, 6608-10, 6613-16, 6620-21, paras. 4, 11, 14, 21-22, 24, 27, 38.

[99] *See* Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, Federal Communications Commission at 1 (Nov. 13, 2019) ("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.").

[100] *See Final Designation Order*, 35 FCC Rcd at 6607-609, 6616-17, paras. 8, 11-12 and 29.

[101] *See id*. at 6620, para. 36.

the expertise of the Cyber Security Evaluation Centre Oversight Board.[102] Huawei failed to rebut or even address the Board's findings in its Application for Review.

30. Huawei did attack the Bureau's use of a 2019 report by Finite State,[103] which similarly concluded Huawei's equipment had security vulnerabilities, but the Bureau was also correct to rely upon that report because it established that Huawei equipment was less secure than that of its competitors and that Huawei was slow to address security problems with its equipment.[104] Technical reports on Huawei equipment also evince concerns that any "technical mitigation techniques" (even sophisticated ones) would be insufficient to protect against Chinese security service exploitation, further buttressing the Commission's concerns with such equipment.[105]

31. We are bolstered in our decision by the actions that a number of other countries, including several major U.S. allies, have taken to restrict or altogether bar the purchase or integration of Huawei equipment and services into network infrastructure because of security vulnerabilities.[106] And a number of European communications providers have also moved to limit or cease business dealings with Huawei altogether.[107] Other countries' and telecommunications providers' own assessments of the exposure to risk within their own networks have driven foreign governments and the telecommunications industry to take seriously the security vulnerabilities currently present in Huawei's equipment and the threat of legal or extralegal coercion by the Chinese government.

32. Huawei claims that the steps taken by U.S. allies and foreign communications providers designating Huawei as a national security risk are based on "non-evidence" and unreliable evidence.[108] We disagree. Huawei misunderstands the nature of the risk assessment the Bureau undertook. The fact that many U.S. allies and European communications providers have reached similar conclusions and taken steps to bar the purchase of or remove Huawei equipment and services from their networks supports the Bureau's determination that Huawei poses a threat to U.S. national security.

33. We find that Huawei's evidentiary challenges are misplaced. The Commission previously addressed 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"[109] and therefore should not have been relied upon by the Bureau. "In assessing risks to national security, conclusions must often be based on informed judgment rather than concrete evidence."[110] Questions involving national security therefore often "'involve the exercise of a discretion demonstrably committed

[102] Hadas Gold, *UK bans Huawei from its 5G network in rapid about-face*, CNN Business (July 14, 2020), https://www.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html.

[103] Huawei AFR at 16-17.

[104] *Final Designation Order*, 35 FCC Rcd at 6619, 6621, paras. 34, 39.

[105] *See* Andy Keiser & Bryan Smith, The National Security Institute, Policy Paper, Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat at 23 (2019), https://nationalsecurity.gmu.edu/chinese-telecommunications/.

[106] *See Final Designation Order*, 35 FCC Rcd at 6617-18, para. 31 (describing actions by Australia, Japan, the European Union, the United Kingdom, and other countries); *see also* Politico, *Sweden bans Huawei, ZTE equipment from key parts of 5G network* (October 20, 2020) (Based upon assessments made by the Swedish Armed Forces and the Swedish Security Service, Swedish authorities banned Huawei equipment in large parts of their 5G networks.).

[107] *Final Designation Order*, 35 FCC Rcd at 6618, para. 32.

[108] Huawei AFR at 8-10.

[109] *Final Designation Order*, 35 FCC Rcd at 6623-24, para. 43.

[110] *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)).

to the executive or legislature.'"[111] For example, the D.C. Circuit has held that, under the Antiterrorism and Effective Death Penalty Act, the question of whether the terrorist activity of an organization threatens the security of the United States was appropriately committed to the Department of State's discretion.[112] Such matters are committed to the discretion of agencies with expertise in the area.[113] As a result, it is entirely appropriate for us to look for guidance to the actions and statements of agencies with expertise in national security issues and members of Congress, as the Commission has done here.[114]

34. 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, the establishment of past conduct requires specific proof. 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.[115] Such "predictive judgments" made by agencies with expertise in the relevant area are entitled to deference.[116] 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,[117] we have 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.

35. Finally, we disagree with Huawei's assertion that the Bureau acted arbitrarily and capriciously or treated Huawei differently than other similarly situated companies in violation of the Administrative Procedure Act.[118] In the *Final Designation Order*, the Bureau supported the final designation based on the overwhelming evidence in the record demonstrating that Huawei should be considered harmful to the country's telecommunications network security. Huawei's arguments are beside the point: We are faced with compelling and specific evidence of the threat Huawei poses to the nation's communications networks. And in any event, there are no similar entities to Huawei (and ZTE, the other entity the Bureau designated). As the House Permanent Select Committee on Intelligence explained in discussing its choice to initially focus its investigation on Huawei, Huawei may not be the only company presenting a risk "but [Huawei and ZTE are] the two largest Chinese-founded, Chinese-owned telecommunications companies seeking to market critical network equipment to the United

[111] *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)).

[112] *People's Mojahedin Org. of Iran v. U.S. Dep't of State*, 182 F.3d 17, 23 (D.C. Cir. 1999).

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

[114] *See, e.g., Holy Land Found. for Relief & Devel. v. Ashcroft*, 333 F.3d 156, 162 (D.C. Cir. 2003) (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.

[115] *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 making a national security designation).

[116] *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 quotations omitted); *SBC Communications v. FCC*, 138 F.3d 410, 421 (D.C. Cir. 1998).

[117] 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.

[118] Huawei AFR at 18.

States."[119] Even if other companies may warrant investigation, that does not preclude us from choosing to proceed against Huawei given the accumulation of evidence in favor of designating it as a security threat. Moreover, Huawei fails to address the fact that since at least 2012, the Executive Branch and Congress have repeatedly expressed serious concerns about Huawei's presence in U.S. communications networks.[120] To the contrary, the Bureau in the *Final Designation Order*—and we in the *Protecting Against National Security Threats Order*—were justified to proceed incrementally in acting to first designate Huawei (and ZTE) before investigating other companies that may pose threats.[121]

B. The Commission Has Sufficient Authority to Designate Huawei

36. We conclude the Commission has sufficient authority to designate Huawei. As an initial matter, the Commission has already addressed Huawei's claims that "the Commission lacked the authority to promulgate the *[Protecting Against National Security Threats] Order*, 47 CFR § 54.9, and to conduct any 'designations' under it."[122] Huawei's purported challenge to the Bureau's legal authority to impose this designation is in fact a challenge to the Commission's underlying authority to issue the rule itself, rather than to the *Final Designation Order*. As such, we deny these challenges to the extent that they constitute an untimely petition for reconsideration.[123] And in any event, Huawei's arguments fail on the merits. As we have already determined, the Commission has independent authority under sections 201(b) and 254 of the Communications Act, as well as under CALEA, to promulgate the underlying rule.

37. We find that the passage of the Secure Networks Act did nothing to limit the scope of the designation or undermine its authority under section 54.9 of our rules to designate Huawei as a security threat. In the Application for Review, Huawei contends that the Secure Networks Act somehow narrows the Commission's authority to protect national security, by limiting its responsibility only to keeping a list of specific equipment excluded from universal service programs.[124] We disagree. Indeed, to the contrary, the Secure Networks Act bolsters our authority to designate Huawei pursuant to section 54.9 in two ways. First, it provides recent evidence and corroboration that Congress and the President continue to see Huawei equipment and services as a national security threat given that Huawei equipment and services are specifically identified in the Secure Networks Act as equipment and services that pose a national security risk.[125] 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 and safety of United States persons."[126]

---

[119] *2012 HPSCI Report* at 8.

[120] *See Protecting Against National Security Threats Order*, 34 FCC Rcd at 11425-27, paras. 6-13.

[121] *Final Designation Order*, 35 FCC Rcd at 6611, para. 16 & n.52 (citing *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.")).

[122] Huawei AFR at 2; *see also Final Designation Order*, 35 FCC Rcd at 6608, para. 10 & n.35.

[123] *See* 47 CFR § 1.429(d) (establishing a petition for reconsideration deadline of 30 days from public notice of the Commission action).

[124] Huawei AFR at n.9.

[125] *See* Secure Networks Act § 2(c)(3); *see also Final Designation Order*, 35 FCC Rcd at 6622, para. 42 & n.148 (citing 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)). In fact, 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. *Final Designation Order*, 35 FCC Rcd at 6624, para. 45.

[126] *Final Designation Order*, 35 FCC Rcd at 6623, para. 43 & n.152 (citing Secure Networks Act § 2(c)(3) (prohibiting equipment listed in the 2019 NDAA such as Huawei's equipment)).

38. Second, section 3(b) of the Secure Networks Act, which was signed into law after the *Protecting Against National Security Threats Order* in which we first initially designated Huawei, explicitly preserves any action, including any designation, that we have already taken that is consistent with the Secure Networks Act.[127] Section 3 of the Secure Networks Act provides additional support for our finding as that newly enacted provision directs the Commission to "implement" a prohibition on using universal service support for covered equipment or services from, among other sources, Huawei.[128] Although section 3 states that the Commission must issue rules to effectuate the Secure Networks Act, Congress specifically provided that the Commission is not compelled to revisit any prior action that is consistent with the Secure Networks Act.[129] Congress's recognition that we may take steps to protect national security under other statutory authorities further supports the position that we had sufficient independent authority to designate Huawei under sections 201 and 254 of the Communications Act, and CALEA.[130] As we recently clarified in the *July Declaratory Ruling*, section 54.9 of the Commission's rules, including the designation process completed with the Bureau's decision, is "consistent" with the Secure Networks Act and fulfills the statutory mandate to implement a ban on USF funds for covered equipment within 180 days of the enactment of the Secure Networks Act.[131] We therefore conclude that the Secure Networks Act does not restrict the Commission's ability to protect our national security by safeguarding our communication networks, including by using our authority over the Fund pursuant to section 254 of the Communications Act.

39. Huawei's invocation of *FDA v. Brown & Williamson*[132] is similarly unpersuasive. In that case, the Supreme Court held that the FDA lacked authority to regulate tobacco products.[133] To the extent that Huawei is arguing that the Communications Act does not support section 54.9 of the Commission's rules, we disagree. The Supreme Court in *Brown & Williamson* relied on the fact that after passing the Food, Drug, and Cosmetic Act, which the FDA argued gave it the power to regulate tobacco as a drug, Congress subsequently passed laws that established a regulatory scheme for tobacco that was inherently at odds with the FDA's regulation of tobacco.[134] That case is inapposite to the instant situation: After the enactment of section 54.9, Congress explicitly granted the Commission independent statutory authority to "implement" a prohibition on using universal service support for covered equipment or services from, among others, Huawei.[135] Unlike in *Brown & Williamson*, here Congress has expressly spoken to the question at issue—and in a manner entirely consistent with the Commission on the issue—passing the Secure Networks Act which provides that Huawei telecommunications equipment and services "pose[] an unacceptable risk to the national security of the United States or the security and safety of United States

[127] Secure Networks Act § 3(b) states, "If the Commission has, before the date of the enactment of this Act, taken action that in whole or in part implements subsection (a), the Commission is not required to revisit such action, but only to the extent such action is consistent with this section." Secure Networks Act § 3(b); *see also Final Designation Order*, 35 FCC Rcd at 6607, para. 6 & n.25.

[128] *Final Designation Order*, 35 FCC Rcd at 6622, para. 40 (citing Secure Networks Act § 3).

[129] Secure Networks Act § 3(b).

[130] *Id*.

[131] *Id*. § 3(a)-(b).

[132] *FDA v. Brown & Williamson*, 529 U.S. 120, 143 (2000).

[133] *Id*. at 143, 161.

[134] *Id*. at 121.

[135] Secure Networks Act § 3(b).

persons,"[136] and directing the Commission to bar the use of universal service support for Huawei telecommunications equipment and services.[137]

C. Huawei Was Not Denied a Fair Process

40. On the issue of fairness and notice, Huawei had ample opportunity to fully participate in the proceedings, both administrative and adjudicative, and was not deprived of due process as it contends. Huawei availed itself of the opportunity to submit numerous comments, including reply comments, and written and oral *ex parte* presentations in the rulemaking and was also able to file responses in this adjudication, including the instant Application for Review.[138] Here, after considering Huawei's numerous submissions in the *Protecting Against National Security Threats* proceeding, the Commission provided notice to Huawei by initially designating it as a covered company and describing the process that would follow to consider finalizing that designation.[139] While the initial designation order repeatedly cited congressional concerns regarding the potential for supply chain vulnerability and the possible risks associated with certain foreign communications equipment providers, the initial designation did not find that Huawei had violated any law and had no binding effect on any party's actions.[140] Before the adoption of the *Final Designation Order*, the only order having legal consequences to Huawei, Huawei had multiple opportunities to respond to the initial designation, and it availed itself of each opportunity.[141] After the initial designation of Huawei, it filed thousands of pages of comments, declarations, and expert reports raising numerous factual and legal arguments.[142] After the Bureau released a public notice seeking comment on the applicability of the Secure Networks Act to this designation proceeding,[143] Huawei again filed comments. Once NTIA submitted the views of the Executive Branch in this proceeding,[144] the Bureau provided yet another opportunity for Huawei to respond,[145] and Huawei filed comments in response to NTIA's filing.[146] Huawei cannot now complain that it did not receive adequate notice.[147]

---

[136] *See id*. § 2(b)(2)(C) & (c)(3) (prohibiting equipment and services listed in the 2019 NDAA, including Huawei's equipment and services).

[137] *See id*. § 3 (directing the Commission to implement a rule banning the use of Federal subsidies for covered communications equipment and services, including Huawei's telecommunications equipment and services).

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

[139] *See Protecting Against National Security Threats Order*, 34 FCC Rcd at 11449, Section III.B.

[140] *See id*. at 11438, 11459-63, paras. 40, 94-103.

[141] *See* Huawei Designation Comments.

[142] *See id*.

[143] *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 and 19-352, 35 FCC Rcd 2072 (PSHSB 2020).

[144] *See* NTIA Letter.

[145] *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 and 19-352, 35 FCC Rcd 5791 (PSHSB 2020).

[146] *See* Huawei NTIA Filing Comments; NTCA NTIA Filing Comments; RWA Comments (filed June 19, 2020); USTelecom NTIA Filing Comments.

[147] The Due Process Clause requires notice and an opportunity to be heard, not endless rounds of notice and hearing. *See, e.g.*, *Crum v. Vincent*, 493 F.3d 988, 993 (8th Cir. 2007) ("So long as one hearing will provide . . . a meaningful (continued….)

Moreover, by initially designating Huawei, the Commission provided Huawei with clear notice that the Bureau was considering whether to finally designate Huawei as a covered entity and gave Huawei every opportunity to show it should not be designated.

41. We reject Huawei's argument that cross-examination was required to "protect against the risk of erroneous deprivation."[148] First, 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 than the proceeding at issue; and second, balancing the three factors in *Mathews v. Eldridge*[149] 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 we and the Bureau relied, making the risk of an erroneous deprivation minimal. Further, the administrative burden of calling the various experts that contributed to the underlying reports would be significant and not justified under the circumstances. In sum, we find that trial-type proceedings were not constitutionally required here, and that the Commission and the Bureau therefore had discretion to choose the form of the proceeding that it would conduct.

42. We also reject Huawei's argument that certain Commissioners prejudged the outcome of this proceeding. Courts have explained that "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]."[150] Here, neither the Chairman nor any other Commissioner made statements suggesting that Huawei's designation was a foregone conclusion. Even if certain Commissioners may have made public statements reflecting their own concerns about Huawei's equipment, there is no indication here that the Chairman or the Commissioners' minds were "irrevocably closed" on whether Huawei should be designated, nor that there was bias in this proceeding.[151] Rather, the Commission, in making its initial designation, presented evidence that indicated the risk Huawei posed and provided Huawei with multiple opportunities to respond. Indeed, the authority over the Huawei designation was delegated to the Bureau to make a final designation based on the totality of the evidence before it.[152] And we arrive at our decision today only after having reviewed a fulsome record and multiple opportunities for Huawei to provide evidence and comment. Other court cases Huawei cites in support of its prejudgment arguments are inapplicable

(Continued from previous page)
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.").

[148] Huawei AFR at 24.

[149] *Mathews v. Eldridge*, 424 U.S. 319 (1976) (establishing a three-factor balancing test for assessing procedural due process claims: (1) the private interest that will be affected by the official action; (2) a cost-benefit analysis of the risks of an erroneous deprivation versus the probable value of additional safeguards; and (3) the Government's interest, including the function involved and any fiscal and administrative burdens associated with using different procedural safeguards). *Id*. at 335.

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

[151] *See FTC v. Cement Institute*, 333 U.S. 683 (1948) (rejecting a claim that FTC Commissioners must disqualify themselves because they had, prior to a hearing on the legality of a pricing scheme, already formed an opinion that the defendants' pricing system was illegal because, among other reasons, the Commissioners could change their minds and the defendants had an opportunity to present their case); *United States v. Batson*, 782 F.2d 1307, 1315 (5th Cir. 1986) (rejecting a claim of prejudgment because "there is no significant evidence to indicate that any hearing officers mind was irrevocably closed, nor is there any evidence from which we could reasonably infer that [the hearing officers were] biased").

[152] *Final Designation Order*, 35 FCC Rcd at 6604, para. 1.

because they involve the question of whether the decisionmaker ignored evidence before it or was personally biased against a party, neither of which is the case here.[153]

43. Finally, Huawei's arguments about congressional pressure are no more persuasive. Correspondence from members of Congress asking an agency to examine a subject is not itself unlawful 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.[154] Huawei claims that the Commission's written response to such concerns demonstrates that the Commission was under pressure from Congress but cites no case law for this proposition.[155] And Congress exerted no pressure on the Commission, such as by threatening to withhold funding, to arrive at a particular outcome.[156] Indeed, the D.C. Circuit has held that holding an adjudicatory proceeding may be an "appropriate response" to such an inquiry by members of Congress.[157]

D. Huawei Was Not Deprived of Its Interests in Liberty or Property

44. For the reasons we explained in the *Protecting Against National Security Threats Order* and the Bureau explained in the *Final Designation Order*, Huawei's designation does not interfere with a cognizable liberty interest.[158] But even if it did, Huawei was given all the process that was due in this proceeding, and we are unconvinced by Huawei's argument that the final designation deprives it of liberty interests protected under the Due Process Clause.[159] As the Commission has already explained, designation under section 54.9 of the Commission's rules does not deny the designated party a property or liberty interest protected by the Due Process Clause.[160]

45. Huawei complains that "being designated a national security threat . . . will discourage *all* potential customers—regardless of whether they are universal service support recipients—from purchasing and using Huawei equipment,"[161] which in Huawei's view creates a denial of a property and liberty interest.[162] Huawei further argues that the final designation would deprive it of property interests, and to support its claim, points to "existing contracts with [universal service] recipients and suppliers to [universal service] recipients," which it claims would be interfered with or "effectively abrogate[d] through the designation process . . . ."[163] We disagree. Huawei ignores long-standing "Commission and

[153] *See Metro Council of NAACP v. FCC*, 46 F.3d 1154, 1164-65 (D.C. Cir. 1995); *Cinderella Careers and Finishing Schools, Inc. v. FTC*, 425 F.2d 583, 590 (D.C. Cir. 1970).

[154] *See* Huawei Supply Chain Comments at 116-17.

[155] *Id*. at 117-18.

[156] *See D.C. Fed'n of Civic Associations v. Volpe*, 459 F.2d 1231, 1246 (D.C. Cir. 1971) (Member of Congress 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 Member of Congress, written after testimony was heard at an agency hearing, that urged a specific outcome found to have compromised the appearance of impartiality).

[157] *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.").

[158] *Final Designation Order*, 35 FCC Rcd at 6627-29, paras. 52-57.

[159] Huawei AFR at 21; *see Protecting Against National Security Threats Order*, 34 FCC Rcd at 11459-63.

[160] *See Final Designation Order*, 35 FCC Rcd at 6627-29, paras. 51-57; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11460, para. 99.

[161] Huawei AFR at 21.

[162] *Id*. at 22.

[163] *Id*.

judicial precedent [that] make[s] clear that carriers have no vested property interest in ongoing . . . support."[164] Indeed, the independent decision of a Universal Service Fund recipient to discontinue its relationship with Huawei does not create a governmental obligation or a contractual right to maintain continuity between private entities. Moreover, Huawei cites no case to support this proposition, and thus, we find that the designation does not impose any explicit restrictions on Huawei's ability to contract with any recipients.

46. To succeed with this claim, Huawei 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'"[165] to establish a denial of a cognizable liberty or property interest. We do not pass on the first prong because Huawei so clearly fails to establish the second prong of the two-prong stigma-plus test. Here, the purported existence of stigma alone is not enough to demonstrate a deprivation. Even if designation creates a "disincentive for carriers to purchase equipment from designated entities," recipients of universal service support may still continue purchasing equipment and services from Huawei without using support from the Fund.[166] Nor does Huawei identify any other concrete legal right that it has been denied.[167] Huawei does not, for example, cite a protected "business goodwill" interest[168] allegedly impacted by designation,[169] nor the loss of a

[164] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11463, para. 105 & n.288.

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

[166] *Final Designation Order*, 35 FCC Rcd at 6627-28, para. 54.

[167] *See Gen. Elec. Co. v. Jackson*, 610 F.3d 110, 121 (D.C. Cir. 2010).

[168] Huawei further claims that the "final designation would debar Huawei from participating in a government program as a supplier of equipment to USF fund recipients . . ." and as a result it alleges that it was deprived of its liberty interests. Huawei AFR at 22-23. It is unclear how Huawei arrives at this conclusion from the *Kartseva v. Dep't of State*, 37 F.3d 1524, 1527 (D.C. Cir. 1994) and *Phillips v. Vandygriff*, 711 F.2d 1217 (5th Cir. 1983) 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. *Kartseva*, 37 F.3d at 1526. 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. *Id.* at 1527. Here, Huawei 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. Contrary to *Kartseva*, the "designation [in Huawei] imposes no explicit restriction on designated entities at all," and indeed Huawei remains "free to sell to anyone, including recipients of USF." *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11462, para. 103; *see also Final Designation Order*, 35 FCC Rcd at 6628-29, para. 56. The second case Huawei cites is equally immaterial. *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. *Phillips*, 711 F.2d at 1217. Notably, the court found "the difference between formal licensing and *de facto* licensing to be unimportant," *(id.* at 1223) and that denying a person credentials that are "practically necessary for pursuing a chosen profession" could represent denial of a liberty interest. *Id*. 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, or how such decision amounts to *de facto* licensing. Accordingly, because the designation imposes no explicit restriction on Huawei and it remains free to sell equipment and services to any carrier, including recipients of USF, and Huawei has not (and could not) adequately support its conclusion that the designation somehow deprives it of a liberty interest, we affirm the Bureau's designation decision.

[169] *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").

"cognizable interest in avoiding the loss of government contracting opportunities."[170] Additionally, the fact that carriers receiving universal service support—let alone service providers not receiving support from the Fund—can continue to contract with Huawei means that a final designation does not reach the level of "broad preclusion" required.[171] And many communications providers do not receive universal service support and are thus unaffected by the final designation. Accordingly, we affirm that the final designation of Huawei as a covered company is appropriate and, as a result, funds from the 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.

IV. ORDERING CLAUSES

47. Accordingly, IT IS ORDERED, pursuant to sections 1, 4(i), 4(j), 5(c), 214, 229, and 254 of the Communications Act of 1934, as amended, and section 105 of the Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 151, 154(i), 154(j), 155(c), 214, 229, 254, 1004, and section 1.115 of the Commission's rules, 47 CFR § 1.115, that this order IS ADOPTED.

48. IT IS FURTHER ORDERED that the Application for Review filed by Huawei Technologies Co. LTD and Huawei Technologies USA, Inc., IS DENIED.

49. IT IS FURTHER ORDERED that, pursuant to section 1.103(a) of the Commission's rules, 47 CFR § 1.103(a), this order SHALL BE EFFECTIVE upon release.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

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

[171] *Id.*; *see, e.g., Gen. Elec. Co.*, 610 F.3d at 121 ("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. Cir. 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*, 314 F.3d at 644-45)).

STATEMENT OF
CHAIRMAN AJIT PAI

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation*, PS Docket No. 19-351.

Just a few minutes ago, we adopted rules requiring certain carriers to remove from their networks equipment that poses a threat to our national security and the integrity of the country's communications networks and implementing the Secure and Trusted Communications Networks Reimbursement Program that will help smaller service providers shoulder the cost of removing and replacing such equipment. Earlier this year, our Public Safety and Homeland Security Bureau issued a final designation of Huawei Technologies Company, along with its parent, affiliate, and subsidiary companies, as a national security threat as part of the Commission's ongoing efforts to protect our nation's communications networks and their supply chains.

And today, we affirm the Bureau's Order designating Huawei as a threat to national security and our nation's communications infrastructure. A laundry list of evidence before us compels this result and is set forth in our decision today. But to summarize some of the main points, Huawei has a long and well-documented history of close ties to the Chinese military and intelligence communities, as well as the Chinese Communist Party, at every level of the company—all the way up to its founder. Huawei is subject to sweeping Chinese intelligence laws compelling Huawei's assistance and cooperation with Chinese intelligence services and forbidding the disclosure of that assistance. Moreover, the concerns about Huawei aren't just hypothetical: Independent entities have identified numerous security vulnerabilities in Huawei equipment and found it to be less secure than that of other companies—perhaps deliberately so.

Our decision today to uphold the Bureau's final designation order will have a direct impact on the security and integrity of the country's networks. Carriers will continue to be unable to use support from the Commission's Universal Service Fund to purchase network equipment or services from Huawei, thus helping to keep its insecure equipment out of our networks.

For their continuing commitment to this ongoing effort, I think the Commission staff that contributed to this item, including: Lisa Fowlkes, Jeffery Goldthorp, Jennifer Holtz, Debra Jordan, Nicole McGinnis, Saswat Misra, Austin Randazzo, and Avery Roselle of the Public Safety and Homeland Security Bureau; Pam Arluk, Rhonda Campbell, Elizabeth Cuttner, Justin Faulb, Charlene Goldfield, Janice Gorin, Trent Harkrader, Kris Monteith, Ramesh Nagarajan, Rachel Nixon, Ryan Palmer, and Jaina Patel of the Wireline Competition Bureau; Aaron Garza of the Consumer and Governmental Affairs Bureau; and Malena Barzilai, Michael Carlson, Matthew Dunne, Thomas Johnson, Douglas Klein, Rick Mallen, Linda Oliver, and Bill Richardson of the Office of General Counsel.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation*, PS Docket No. 19-351.

When this Commission began the process of securing America's communications networks against the threats posed by bad actors, we followed the evidence. And when it comes to Huawei, there is certainly plenty of it. Starting back in 2012, the House Permanent Select Committee on Intelligence issued a report recommending that companies avoid using Huawei equipment and that government agencies remain vigilant and focused on the threat. Several National Defense Authorization Acts have continued to sound the alarm, banning federal agencies from using this potentially dangerous equipment.

The FCC's review aligns with those recommendations. Our record shows that Huawei is effectively under the control of the Communist Party of China. And it has engaged in a wide range of nefarious activities, including working in support of the surveillance and detention of over a million Uighurs in Xinjiang—efforts it undertakes in conjunction with the Xinjiang Public Security Bureau. Huawei's entanglement with Communist China's surveillance state does not end there. It has close ties to the People's Liberation Army, and the Ministry of State Security. In fact, China's National Intelligence Law even requires them to "cooperate with the State intelligence work," and it provides them no right to refuse. It also gives the Chinese government the power to take over a company's communications equipment.

The threats posed by the Communist Party's control over Huawei are not theoretical. Just last year, a grand jury returned an indictment alleging that Huawei had stolen trade secrets from a U.S. carrier. Comprehensive studies have also shown security vulnerabilities in Huawei equipment—defects in their software engineering and cybersecurity processes that are so severe even sophisticated technical mitigation techniques would be insufficient to fix them. The record also shows the Chinese government has been able to influence Huawei's design and manufacturing processes.

I am grateful for the leadership that Chairman Pai has shown in confronting the threat posed by Huawei. In collaboration with our State Department partners, Chairman Pai and his team have not only worked to protect America's networks, they have ensured that our allies abroad do not allow insecure gear to proliferate in their networks. Today, Australia, the Czech Republic, Japan, Sweden, and the U.K. among others have reached the same conclusions that we have in the U.S. We should treat Huawei as nothing short of a threat to our collective security. Because this decision does so, it has my support.

Thank you to the staff of the Wireline Competition Bureau and Public Safety and Homeland Security Bureau for their hard work on this important item.