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. 19-352
Programs – ZTE 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 ZTE Corporation (ZTE). 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 ZTE, as covered companies for the purposes of this rule, and 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 ZTE, 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

[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*).

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

[3] 47 CFR § 54.9(a).

Service Fund may no longer be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by ZTE.

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 ZTE and Huawei Technologies Company (Huawei) as covered companies for purposes of its rule.[10] The Commission initially designated ZTE and Huawei because it found that they 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 ZTE's ties to the Chinese government and military apparatus,[12] 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.[13] The

[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 C.F.R. § 54.9*, PS Docket Nos. 19-351 and 19-352, Public Notice, DA 20-471 (PSHSB 2020) (*Designation Extension Public Notice*).

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

[11] *Order*, 34 FCC Rcd at 11441, para. 43-46.

[12] *Order*, 34 FCC Rcd at 11447-48, para. 60.

[13] *See Order*, 34 FCC Rcd at 11440-41, paras. 45-46.

Commission also relied on reports highlighting known cybersecurity risks and vulnerabilities in ZTE equipment, which has led a number of countries to bar the use of such equipment.[14] Furthermore, the Commission was informed by the steps taken by Congress and the Executive Branch to restrict the purchase and use of ZTE equipment, including the Department of Defense's decision to remove ZTE devices from sale at U.S. military bases and from its stores worldwide.[15] The Commission also relied on evidence of ZTE's disregard for American law, including ZTE's violation of the U.S. embargo on Iran by sending approximately $32 million of U.S. goods to Iran and obstructing justice in the Department of Justice's investigation.[16]

5. After the initial designation of ZTE, 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] ZTE filed comments opposing the initial designation and urging us not to finalize it.[19] In particular, ZTE asserts that it has made progress in two areas: (1) compliance with U.S. export controls; and (2) cybersecurity in its products and services.[20] In both areas, ZTE argues that it has "adopted export compliance practices with a focus on People, Process, Technology and Industry Outreach."[21] ZTE did not respond to the other findings made by the Commission.[22]

6. Recently, on March 12, 2020, the President signed into law the Secure and Trusted Communications Networks Act of 2019 (the Secure Networks Act).[23] 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

---

[14] *Order*, 34 FCC Rcd at 11448, para. 61 (citing Kryptowire, *Vulnerable Out of the Box: An Evaluation of Android Carrier Devices*, at 1 (Aug. 10, 2018), https://www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf); *see also* Kryptowire, *DEFCON 2018: Vulnerable Out of the Box – An Evaluation of Android Carrier Devices* (Aug. 10, 2018), https://www.kryptowire.com/android-firmware-defcon-2018/; Justin Lynch, *New research says ZTE phones could be hacked*, Fifth Domain (Aug. 9, 2018), https://www.fifthdomain.com/show-reporters/black-hat/2018/08/10/new-research-says-zte-phones-could-be-hacked/; Andy Keiser & Bryan Smith, The National Security Institute, Policy Paper, *Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat* at 2 (2019), https://nationalsecurity.gmu.edu/chinese-telecommunications/.

[15] *Order*, 34 FCC Rcd at 11447-48, paras. 60-61; *see* National Defense Authorization Act for Fiscal Year 2018, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656 (2018 NDAA); 2019 NDAA, 132 Stat. 1917, Sec. 889; Phil Stewart & Jeffrey Benkoe, *Pentagon stops selling Huawei, ZTE phones in its bases, cites security*, Reuters (May 2, 2018), https://www.reuters.com/article/us-usa-china-huawei-tech/pentagon-stops-selling-huawei-zte-phones-in-its-bases-cites-security-idUSKBN1I326H.

[16] *Order*, 34 FCC Rcd at 11448, para. 62 (citing Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, Federal Communications Commission, WC Docket No. 18-89, at 1-2 (filed Nov. 14, 2019) (DoJ Letter)).

[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 (Jan. 3, 2020).

[19] *See generally* ZTE Comments. Additionally, we received one express comment filed by an individual in the Commission's Electronic Comment Filing System that opposed ZTE's designation as a covered company. Several other filings in PS Docket No. 19-352 were also filed in WC Docket No. 18-89 and did not relate to the ZTE designation, so we do not address them here.

[20] ZTE Comments at 2.

[21] ZTE Comments at 2-5.

[22] *Id.* at 1-2.

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

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 ZTE or its subsidiaries and affiliates,[24] so long as the equipment or service is capable of 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.[25] 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.[26]

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.[27] In response, ZTE argues that we should not finalize the initial designation and should instead implement the Secure Networks Act.[28]

8. Finally, on June 9, 2020, the National Telecommunications and Information Administration (NTIA) submitted a filing in the docket stating that the Executive Branch "fully supports" the initial designations of ZTE and Huawei and providing the Executive Branch's analysis of matters including the legal framework in China, the national security risks posed specifically by ZTE and Huawei, and the national security interests demonstrated by their violations of U.S. law.[29] The Bureau provided an opportunity for ZTE and other interested parties to respond by seeking comment on this filing on June 9, 2020.[30] Three parties filed comments in response to NTIA's filing.[31] ZTE did not file any comments.

---

[24] *See* Pub. L. 115-232, 132 Stat. 1918, Sec. 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).

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

[26] *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).

[27] *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) (Secure Networks Act PN).

[28] ZTE Secure Networks Act PN Comments at 2. In its comments on the Secure Networks Act PN, RWA reiterates its concerns about the timing of a designation and argues that "the Commission should abstain from issuing any final designation public notice before March 2021." RWA Secure Networks Act PN Comments at 4. USTelecom argues that ZTE should be designated pursuant to the Secure Networks Act, but that the type of prohibited equipment should be limited only to that equipment listed in the Secure Networks Act. *See* USTelecom Secure Networks Act PN Comments.

[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).

[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) (NTIA Letter PN).

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

III. DISCUSSION

9. We issue this final designation of ZTE 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. 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.[33] We conclude that, based on the reasoning supporting the Commission's initial designation and an assessment of the totality of evidence before us, including ZTE's filings in response to the initial designation, ZTE poses a national security threat to our nation's communications networks and communications supply chain.[34] Accordingly, USF recipients may not use USF funds to purchase, obtain, maintain, improve, modify, or otherwise support equipment or services from ZTE or its subsidiaries, affiliates, and parents in any way, including upgrades to existing ZTE equipment and services.[35]

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

10. In the *Order*, the Commission identified ZTE as posing a 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 surveillance.[36] The *Order* also noted that Chinese law does not meaningfully restrain the Chinese government because of that government's "authoritarian nature, lack of sufficient judicial checks, and its history of industrial espionage."[37] The Commission further cited evidence of ZTE's history of non-compliance with U.S. export and trade laws and known security flaws in ZTE's equipment, which has led the United States and some of its allies to significantly restrict the purchase and integration of ZTE equipment and services into their respective communications infrastructure.[38]

11. After careful consideration of the record in this proceeding, we conclude that ZTE poses a national security threat to the integrity of communications networks and the communications supply

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

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

[34] 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 ZTE 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; s*ee also* 47 U.S.C. § 154(j) ("The Commission is authorized to withhold publication of records or proceedings containing secret information affecting the national defense."). This classified information remains a part of the record in this proceeding and provides further support for this final designation.

[35] 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.

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

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

[38] *Order*, 34 FCC Rcd at 11447-48, paras. 59-63.

chain. This conclusion rests on our findings regarding ZTE's close ties to the Chinese government and obligations under Chinese law, ZTE's disregard for U.S. national security laws, known cybersecurity risks and vulnerabilities in ZTE equipment, and ongoing Congressional and Executive Branch concern about such equipment. Moreover, in its comments opposing the initial designation, ZTE does not refute or address many of the Commission's findings in the initial designation regarding the company's current threat to the security of our nation's communications networks and the communications supply chain. Therefore, these initial findings about the risk that ZTE poses to our communications networks and the communications supply chain remain valid and support the final designation we adopt today.

1. ZTE's Close Ties to the Chinese Government and Obligations Under Chinese Law

12. 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.[39] 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,"[40] and there exists a "substantial body of evidence" about the risks of certain equipment providers like ZTE.[41] International experts have found that China has a "notorious reputation for persistent industrial espionage, and in particular for the close collaboration between government and Chinese industry."[42] 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."[43]

13. We also agree with the Commission's finding that ZTE poses a particular security risk because Chinese intelligence agencies have opportunities to tamper with its products in both the design and manufacturing processes.[44] As the U.S. Attorney General has argued in this proceeding, "a

---

[39] *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.

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

[41] *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).

[42] *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)).

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

[44] *See Order*, 34 FCC Rcd at 11440-41, para. 45. *See also 2012 HPSCI Report* at 3 (observing that during product development, "malicious hardware or software [could be] implant[ed] into critical telecommunications components and systems").

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.[45]

14. *ZTE has particularly close ties to the Chinese Government*. ZTE's ties to the Chinese government, along with its obligations under Chinese law, pose a threat to the security and integrity of our communications networks. The Commission's initial designation highlighted concerns about ZTE's ties to the Chinese government, military, and Communist Party, which ZTE does not deny or address in its comments.[46] As explained in the *Order*, the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government—including state intelligence agencies—to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information.[47] ZTE originated from the Ministry of Aerospace, a Chinese government agency,[48] and is owned in part by the Chinese government.[49] Additionally, despite changes to ZTE's board of directors, implemented as a result of its export control settlement with the U.S. Department of Commerce, scholars view the changes to the board with skepticism, "since any director will have close ties to the Chinese government."[50] Indeed, as the Executive Branch points out, "maintaining a good relationship with the [Chinese Communist Party] is a prerequisite for business success," in China.[51] Even more, ZTE serves a hybrid of "commercial and military needs," with much of its ownership consisting of state-owned enterprises and the presence, as required by Chinese law, of an internal Communist Party Committee.[52] We find that ZTE's close ties to the Chinese government create a significant risk that ZTE would comply, voluntarily or through coercion, with Chinese government espionage activity.

---

[45] *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.").

[46] *Order*, 34 FCC Rcd at 11439-41, 11447-48, paras. 43-46, 60.

[47] *Order*, 34 FCC Rcd at 11441, para. 46. *See* Mannheimer Swartling, Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities (2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.

[48] 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 38 (Oct. 8, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf (*2012 HPSCI Report*).

[49] NATO Cooperative Cyber Defence Centre of Excellence, "Huawei, 5G, and China as a Security Threat," at 9 (2019), https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf (NATO Cyber Defence Paper).

[50] Julia Horowitz, *ZTE shakes up management as part of deal with United States*, CNN Business (June 29, 2018), https://money.cnn.com/2018/06/29/news/companies/zte-board-shakeup/index.html (discussing ZTE's actions to remove fourteen members from ZTE's board of directors and replace them with eight new directors elected at the company's annual meeting). *See also id.* ("The controlling entity here is the Chinese state . . . . It's not who's on the board.") (internal quotations omitted); Richard Chirgwin, *ZTE remakes board as demanded by USA*, The Register (July 2, 2018) https://www.theregister.co.uk/2018/07/02/zte_appoints_new_board/ ("Five of the new appointees [to ZTE's board of directors] were either internal promotions, or were associated with ZTE shareholders 'owned by China's Communist Party.'").

[51] NTIA Letter at 7.

[52] *2012 HPSCI Report* at 38-40. *See also id.* at 44 ("the [House Permanent Select Committee on Intelligence] cannot allay concerns that ZTE is aligned with Chinese military and intelligence activities or research institutes").

15. ZTE did not challenge the Commission's determinations with respect to its ties to the Chinese government, nor did it challenge the Commission's interpretation of the Chinese National Intelligence Law. We reiterate the Commission's findings that ZTE is subject to the Chinese National Intelligence Law and subject to the Chinese legal regime generally, which, when combined with ZTE's history of violating U.S. national security laws and close ties to the Chinese government, presents a great risk to the security of our nation's communications networks and communications supply chain.[53]

16. *ZTE'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.[54] ZTE, 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."[55] Because of China's "notorious reputation for persistent industrial espionage," particularly involving close collaboration between the Chinese government and Chinese industry,[56] 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 ZTE 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."[57]

17. 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 ZTE 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.[58] In a similar vein, Article 14 of the 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

[53] *See Order*, 34 FCC Rcd at 11446, para. 56 ("While we recognize that the [Chinese National Intelligence Law] may be interpreted in different ways, the fact remains that entities … that are subject to the [Chinese National Intelligence Law], and subject to the Chinese legal regime generally, pose too great a risk to the security of communications networks and the communications supply chain.").

[54] *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").

[55] RWR 2019 Report at 23.

[56] 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).

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

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

equipment.[59] 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."[60] 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.[61] 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.[62] As the Executive Branch has explained in the record, "[t]aken together, these laws empower the [Chinese] government to make extensive, affirmative demands on Chinese companies and their officers and employees to advance the [Chinese Communist Party's] intelligence gathering interests."[63] The Executive Branch has also 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."[64] 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 ZTE are beholden to the legal and extralegal controls of the Chinese government and Chinese Communist Party.[65] 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 ZTE USA, Inc., 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.

18. ZTE did not dispute the Commission's interpretation of Chinese national security laws. We credit the Commission's and Executive Branch's analysis of the Chinese National Intelligence Law and the Chinese legal regime generally, particularly the Executive Branch's determination that ZTE is

[59] 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.

[60] 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").

[61] 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.

[62] 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).

[63] NTIA Letter at 5.

[64] NTIA Letter at 5.

[65] 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).

beholden to the legal and extralegal controls of the Chinese government and Chinese Communist Party,[66] and thus we cannot conclude that there are sufficient constraints on either the political or legal ability of the Chinese government and the Communist Party to influence or coerce ZTE. When combined with ZTE's demonstrated willingness to not only ignore, but attempt to circumvent United States laws, we conclude that ZTE poses a national security risk to our communications networks and supply chain.

2. ZTE's Disregard for United States National Security Laws

19. We find that ZTE's history of breaking U.S. law and obstructing U.S. investigations continues to support a finding that ZTE poses a threat to the integrity of our nation's communications infrastructure and communications supply chain. In the *Order*, the Commission cited ZTE's history of non-compliance with U.S. laws as evidence of the danger posed by the presence of ZTE equipment in our national communications networks and communications supply chain.[67] As explained by the Department of Justice in support of the Commission's initial designation, ZTE pleaded guilty in 2018 to violating U.S. sanctions by sending approximately $32 million of U.S. goods to Iran and obstructing the Department of Justice's investigation into the matter.[68] The Executive Branch has further explained that "both ZTE and Huawei poses a risk to U.S. national security based on their activities in violation of U.S. law. ZTE has pleaded guilty to engaging in a multi-year conspiracy to supply, build, and operate telecommunications networks using U.S.-origin equipment in violation of the U.S. trade embargo on Iran, and committing hundreds of U.S. sanctions violations involving the shipment of telecommunications equipment. Moreover, ZTE also made false statements and obstructed justice by creating an elaborate scheme to prevent disclosures to and mislead the U.S. Government."[69] The Executive Branch also points out that, "[e]ven after the guilty plea, ZTE continued to make false statements to U.S. authorities and pursuant to a June 2019 settlement agreement with the Bureau of Industry and Security (BIS) agreed to pay $1 billion in penalties."[70]

20. ZTE's violation of U.S. trade agreements and export laws, coupled with its obstruction of the Department of Justice's investigation, indicate a clear disregard for U.S. law and national security. We therefore find unavailing ZTE's argument that its settlement with the Department of Justice is in itself evidence of progress it has made in compliance with U.S. export laws.[71] As the Department of Justice told the Commission, "[s]urely a willingness to break U.S. law combined with a determination to avoid the consequences by obstructing justice argues against the reliability of a provider."[72] Such caution is especially warranted when the laws in question pertain to U.S. national security and when the entity in question has shown a willingness to obstruct the investigations into such national security threats.[73]

---

[66] 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).

[67] *Order*, 34 FCC Rcd at 11448, para. 62.

[68] DoJ Letter at 1-2.

[69] NTIA Letter at 8.

[70] NTIA Letter at 8.

[71] *See* ZTE Comments at 2-4.

[72] DoJ Letter at 2. *See also* NTIA Letter at 8.

[73] We are thus unpersuaded by ZTE's argument that, because it is not currently listed by the Departments of Commerce or Treasury for export control or sanctions restrictions, we should not issue this designation. *See* ZTE Comments at 2.

21. We also find ZTE's claims of improved compliance vis-à-vis its "updated global export control compliance program" do not deserve significant weight in our consideration of the totality of the evidence.[74] ZTE points to its engagement with a variety of internal and third-party compliance standards, best practices, and committees to demonstrate its commitment to export compliance.[75] While such updated export compliance procedures may be a sign of progress, it is not sufficient in itself to counteract ZTE's knowing violations of U.S. national security laws and its proven lack of cooperation in dealing with U.S. criminal investigators. Such history demonstrates a willingness to flout U.S. laws that mere participation in an international organization is insufficient to rebut.

3. Known Cybersecurity Risks and Vulnerabilities in ZTE Equipment

22. We also find that security risks and vulnerabilities in ZTE's equipment pose a threat to the integrity of communications networks and the communications supply chain. As explained in the Commission's initial designation, various reports identify a wide range of vulnerabilities and cybersecurity risks found in ZTE equipment, which have led to an increase in restrictions placed upon its availability in the U.S. market.[76] These concerns relate not only to the security vulnerabilities existent in ZTE technology, but to the insufficiency of technical mitigation techniques in providing "a level of trust for the U.S to protect its networks against the Chinese security services."[77] In response to these concerns, among other things, Congress has passed, and the President has signed into law, three separate bills restricting the government's purchase, use, and funding of ZTE equipment.[78] In February 2018, the leaders of all six top U.S. intelligence agencies warned against purchasing products or services from ZTE or Huawei, 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."[79] And in April 2018, the Department of

---

[74] *See* ZTE Comments at 2.

[75] ZTE Comments at 2-4 (asserting that ZTE has created the Export Control Compliance Committee under the ZTE Board and the Compliance Management Committee, building an export control compliance program, and implementing the SAP Global Trade Systems software in some of its businesses). One organization ZTE specifically identifies is the National Compliance Committee of the China Council for the Promotion of International Trade (CCPIT). ZTE Comments at 3. However, according to one expert, while CCPIT is presented internationally as outside the CCP party-state structure, it "is functionally related to the finance and economics system, linked to the Ministry of Commerce," and in effect, "CCPIT's activities are carried out on behalf of the government and under its guidance." Jichang Lulu, *Repurposing democracy: The European Parliament China Friendship Cluster*, Sinopsis: China in Context and Perspective at 24 (Nov. 26, 2019), https://sinopsis.cz/wp-content/uploads/2019/11/ep.pdf.

[76] *Order*, 34 FCC Rcd at 11448, para. 61. *See* Kryptowire, *Vulnerable Out of the Box: An Evaluation of Android Carrier Devices*, at 1, 4-7, Tbls. 1-2 (Aug. 10, 2018), https://www.kryptowire.com/portal/wp-content/uploads/2018/12/DEFCON-26-Johnson-and-Stavrou-Vulnerable-Out-of-the-Box-An-Eval-of-Android-Carrier-Devices-WP-Updated.pdf (finding a wide range of vulnerabilities in a number of mobile devices manufactured and marketed by ZTE, including those built into the phones during the manufacturing process that could allow malicious access to the data); Andy Keiser & Bryan Smith, The National Security Institute, Policy Paper, *Chinese Telecommunications Companies Huawei and ZTE: Countering a Hostile Foreign Threat* at 2 (2019), https://nationalsecurity.gmu.edu/chinese-telecommunications/ (describing the underlying risks posed by both Huawei and ZTE systems and recommending "additional restrictions on Huawei and ZTE products and services in the U.S.").

[77] *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/.

[78] *See* 2018 NDAA, Pub. L. 115-91, 131 Stat. 1283, 1762, Sec. 1656; 2019 NDAA, 132 Stat. 1917, Sec. 889; Secure Networks Act, §§ 2-3.

Defense announced that ZTE devices would no longer be offered for sale at U.S. military bases and ordered them removed from its stores worldwide.[80]

23. U.S. allies have also responded to risks associated with ZTE by barring ZTE's equipment from their communications infrastructure and supply chain. To date, the United Kingdom, Japan, and Australia have banned or severely restricted the use of ZTE equipment.[81] The Czech Republic's National Cyber and Information Security Agency issued warnings based on its findings and the findings of its allies that "system administrators in critical information infrastructure, whether in the state or private sector, should take adequate measures" against the threat posed by Chinese communications equipment suppliers such as ZTE.[82] An Italian parliamentary security committee urged caution and recommended that the Italian government consider preventing Chinese telecommunications firms such as ZTE from building domestic 5G networks and implement additional measures to protect existing networks from companies with links to foreign governments, including ZTE.[83] These and similar assessments by other countries provide additional evidence that it is more than reasonable to take seriously the risks that ZTE poses to the integrity of the communications supply chain and communications infrastructure.[84]

24. Despite ZTE's statements about adopting industry standards and best practices in order to "provid[e] secure and trustworthy products and services for [its] customers,"[85] ZTE does not dispute the reports of security risks and vulnerabilities identified in its products. Of course, a manufacturer may be able to show that it can remedy security vulnerabilities in its equipment. In this case, however, we consider security vulnerabilities alongside the totality of the evidence—including ZTE's close ties to the Chinese government and its legal obligations under Chinese law, U.S. and allied intelligence agencies' repeated warnings about ZTE equipment, and ZTE's history of disregard for U.S. national security laws. We therefore find that such cybersecurity risks present a national security threat to the integrity of communications networks and the communications supply chain.

4. Ongoing Congressional and Executive Branch Concern About ZTE Equipment

25. Finally, we find that continuing Congressional and Executive Branch concern about ZTE's risk to U.S. national security further supports our findings today. As discussed in the *Order*, both Congress and the Executive Branch have repeatedly stressed the dangers posed by ZTE equipment and

(Continued from previous page)

[79] *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#.

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

[81] *See* Elena Pavlovska, *UK allows limited 5G rule for Huawei, bans ZTE*, New Europe (Jan. 28, 2020), https://www.neweurope.eu/article/uk-allows-limited-5g-role-for-huawei-bans-zte/; Yoshiyasu Shida, Yoshifumi Takemoto, *Japan government to halt buying Huawei, ZTE equipment: sources*, Reuters (Dec. 6, 2018), https://uk.reuters.com/article/us-japan-china-huawei/japan-government-to-halt-buying-huawei-zte-equipment-sources-idUKKBN1O600X; Catherine Shu, *Australia bans Huawei and ZTE from supplying technology for its 5G network*, TechCrunch (Aug. 23, 2018), https://techcrunch.com/2018/08/22/australia-bans-huawei-and-zte-from-supplying-technology-for-its-5g-network/.

[82] Robert Muller, *Czech cyber watchdog calls Huawei, ZTE products a security threat*, Reuters (Dec. 17, 2018), https://www.reuters.com/article/us-czech-huawei/czech-cyber-watchdog-calls-huawei-zte-products-a-security-threat-idUSKBN1OG1Z3 (internal quotations omitted).

[83] B. Lana Guggenheim, *Questions Over Cyber Security Cause Uncertainty in Europe*, South EU Summit (Jan. 13, 2020), https://www.southeusummit.com/europe/questions-over-cyber-security-cause-uncertainty-in-europe/.

[84] *See Order*, 34 FCC Rcd at 11444-43, para. 53 & n.160.

[85] ZTE Comments at 4.

services and have taken numerous actions to mitigate this threat.[86] 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."[87] 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),[88] which prohibits executive agencies from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a substantial or essential component of any system, or as critical technology as part of any system.[89] Section 889(f)(3) of the 2019 NDAA subsequently and generally defines "covered telecommunications equipment or services," as relevant here, as telecommunications equipment produced ZTE or any subsidiary or affiliate of such entities.[90]

26. Moreover, since the time the Commission issued its initial designation of ZTE, 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 ZTE's equipment and services continue to pose to the security and integrity of U.S. communications networks.[91] Our action today designating ZTE as a national security threat to our communications networks and supply chain and the subsequent ban on the use of USF funds to purchase, lease, or otherwise obtain or maintain ZTE 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. 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, ZTE.[92]

27. We are also unpersuaded by arguments that the Secure Networks Act requires us to limit the scope of this designation.[93] 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. As stated above, 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, ZTE.[94] Sections 2(b)(1) and 2(c)(3) of the Secure Networks Act provide

---

[86] *See Order*, 34 FCC Rcd 11425, para. 6.

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

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

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

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

[91] *See* Secure Networks Act § 2(c)(3) (prohibiting equipment from companies, such as ZTE, 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 ZTE); 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).

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

[93] *See* WTA PN Comments at 2; USTelecom PN Comments at 3; ZTE PN Comments at 3; RWA NTIA Filing Comments at 4.

[94] *See* Secure Networks Act § 3. *See also* USTelecom Secure Networks Act PN Comments at 2 (noting ZTE is properly designated as a manufacturer of covered equipment under the Secure Networks Act).

that telecommunications equipment and services produced or provided by ZTE, 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."[95] 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.[96] 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.[97] Indeed, the Secure Networks Act explicitly preserves any action the Commission has already taken that is consistent with the Secure Networks Act.[98]

28. 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.[99] 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.[100] Noting that malware and vulnerabilities can be built directly into equipment,[101] 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."[102] 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.[103] 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 ZTE equipment and services, including that reflected by the enactment of the Secure Networks Act, supports a final designation of ZTE as a covered company for purposes of the Commission's rule.

B. Effective Date

29. The final designation of ZTE Corporation is effective immediately upon release of this Order. We conclude that the risks to our national communications networks and communications supply

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

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

[97] *See id.* at § 2(b)(2)(A)-(B).

[98] Secure Networks Act § 3(b).

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

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

[101] *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)).

[102] *Id*.

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

chain posed by ZTE's equipment necessitate immediate implementation of our designation.[104] 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.

30. We decline to grant requests by ZTE and the Rural Wireless Association (RWA) to further delay adoption of our final designation.[105] ZTE requests that the Commission "take additional time in order to consider additional information" relevant to our final designation.[106] ZTE and other interested parties were granted sufficient time to provide such additional information to the record,[107] and the Bureau has had sufficient time to assess and consider that information.[108] Furthermore, the national security implications associated with our final designation of ZTE weigh in favor of an immediate designation.[109] Lastly, we see no reason to delay any final determination of ZTE until such time as a reimbursement mechanism is established.[110] 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.[111] Additionally, this designation does not require any USF recipient to remove and replace existing equipment. Rather, the effect of this designation is to prohibit the future use of USF support to purchase, obtain, maintain, improve, modify, or otherwise support any such equipment or services. While we recognize that prohibiting the use of USF funds for ZTE 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 support to be used to fund equipment and services that threaten our national security.[112] We therefore see no reason to delay today's designation of ZTE.

---

[104] *Order*, 34 FCC Rcd at 11483, paras. 168-69. As explained in the *Order*, the prohibition of the use of USF funds to procure ZTE 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.

[105] *See* RWA Comments at 1; ZTE Comments at 1-2; RWA Secure Networks Act PN Comments at 1, 4; WTA Secure Networks Act PN Comments at 2; USTelecom Secure Networks Act PN Comments at 3; RWA NTIA Filing Comments at 4.

[106] ZTE Comments at 1-2.

[107] Consistent with the requirements of the *Order*, commenters were provided an initial period of 30 days after publication in the Federal Register to submit responsive comments to the initial designation. *See Order*, 34 FCC Rcd at 11449, para. 65. Commenters had further time to submit comments in response to Bureau-level public notices on the applicability of the Secure Networks Act, and on the NTIA Letter. *See* Secure Networks Act PN; NTIA Letter PN.

[108] Indeed, the Bureau extended the time to finalize the designations for nearly two months to, among other reasons, "fully and adequately consider[] the records in these proceedings." *Designation Extension Public Notice* at 2.

[109] *See Order*, 34 FCC Rcd at 11483, paras. 168-69 (determining that the national security implications necessitate the immediate implementation of the Report and Order and initial designations and finding good cause to expedite the implementation of the rules to make them effective upon publication in the Federal Register).

[110] *See* RWA Comments at 1; RWA Secure Networks Act PN Comments at 1; ZTE Comments at 1-2; ZTE Secure Networks Act PN Comments at 2; RWA NTIA Filing Comments at 3.

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

[112] *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

31. 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 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 M. Fowlkes
Chief
Public Safety and Homeland Security Bureau