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 – ZTE Designation	)	PS Docket No. 19-352

MEMORANDUM OPINION AND ORDER

Adopted: November 24, 2020 **Released: November 24, 2020**

By the Chief, Public Safety and Homeland Security Bureau:

I. INTRODUCTION

1. Last year, the Commission took decisive action to protect America's communications networks and the communications supply chain by adopting 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] In the *Protecting Against National Security Threats Order*, the Commission initially designated ZTE Corporation, along with its parents, affiliates, and subsidiaries (ZTE), as a covered company for the purposes of the rule based on the substantial body of evidence about the risks posed by ZTE to the security of US communications networks. The Commission directed the Public Safety and Homeland Security Bureau (Bureau) to determine whether to issue a final designation of ZTE.[2]

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

3. In response to our final designation, ZTE filed a Petition for Reconsideration (Petition) under section 1.106 of the Commission's rules.[4] Upon review of the record and the Petition, we find no basis for reconsideration and deny ZTE's Petition. Denial furthers the Commission's objective of promoting safe and reliable networks.

II. BACKGROUND

4. 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

[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*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB June 30, 2020) (*Final Designation Order*). *See also* 47 CFR § 54.9(a).

[4] Petition of ZTE for Reconsideration, PS Docket No. 19-352 (filed Jul. 30, 2020) (Petition); 47 CFR § 1.106.

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, on November 22, 2019, the Commission 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] In adopting the rule, the Commission determined that it had independent legal authority to prohibit USF recipients from spending public funds from the USF on covered equipment and services.

5. Following an extensive examination of the record, in the *Protecting Against National Security Threats Order*, the Commission initially designated ZTE as a covered company.[7] It did so because it found that ZTE posed “a unique threat” to the security and integrity of the nation’s communications networks and communications supply chain in light of their size, its close ties to the Chinese government, and the security flaws identified in its equipment.[8] The Commission noted that ZTE’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 non-adherence to the law in any event, make it susceptible to Chinese governmental pressure to participate in espionage activities.[9] The Commission also relied on reports highlighting known cybersecurity risks and vulnerabilities in ZTE equipment, which have led other countries to bar the use of such equipment.[10] 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.[11] The Commission further explained that ZTE had pleaded guilty to violating the U.S. embargo on Iran and further obstructed justice to thwart any U.S. investigations.[12] The Commission directed the Bureau to implement the next steps in the process.[13]

6. On January 3, 2020, we opened this proceeding and sought comment on whether ZTE should be finally designated.[14] 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 designations of Huawei and ZTE and providing the Executive Branch’s analysis of the legal framework in China, the national security risks posed specifically by Huawei and ZTE, and the national security concerns demonstrated by their violations of U.S. law.[15] We

[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] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11439-40, para. 59.

[8] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11447-48, paras. 60-61.

[9] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11447-48, paras. 60-61.

[10] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11448, para. 61.

[11] *Id.*

[12] *Id.*

[13] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11449, para. 64.

[14] *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*, Public Notice, PS Docket No. 19-352, 35 FCC Rcd 292 (PSHSB 2020).

[15] *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 (continued….)

immediately provided an opportunity for ZTE and other interested parties to respond to NTIA's filing in a Public Notice.[16]

7. In the *Final Designation Order*, the Bureau determined that the record supported final designation of ZTE as a national security threat to America's communications networks and the communications supply chain.[17] In support of this determination, we found that ZTE would be compelled under Chinese law to assist with Chinese espionage activities.[18] Moreover, we found that the Chinese Government has strong control over its commercial entities like ZTE and it would likely require that these entities comply with requests from its intelligence agencies, regardless of whether such requests complied with Chinese law.[19] We also found that ZTE has disregarded U.S. national security laws by obstructing U.S. investigations and violating export laws.[20] Finally, we determined there are security risks and vulnerabilities in ZTE equipment that have not been completely addressed.[21]

8. On July 30, 2020, ZTE filed a Petition for Reconsideration of the *Final Designation Order* pursuant to section 1.106 of the Commission's rules. In its Petition, ZTE poses several arguments against its designation as a covered company. First, ZTE argues that the *Final Designation Order* contradicts the congressional intent of the Secure Networks Act. Second, ZTE claims that the Bureau did not consider all available evidence when it concluded that ZTE did not dispute the assertions made regarding the security of its products. Lastly, ZTE contends the Bureau was incorrect to dismiss ZTE's new efforts to comply with U.S. law. The Bureau issued a Public Notice on the filing.[22]

III. DISCUSSION

9. We deny ZTE's Petition because it relies on arguments that have already been considered and rejected by the Bureau and does not demonstrate that the Bureau committed any material error or omission in its analysis. In general, reconsideration is appropriate only when the petitioner demonstrates a material error or omission in the underlying order or raises additional facts not known or not existing until after the petitioner's last opportunity to present such matters.[23] Because ZTE fails to demonstrate that any of these situations are present in the *Final Designation Order*, we deny ZTE's Petition. To the extent that ZTE raises new or expanded arguments, we deny those arguments herein.

(Continued from previous page)
Letter). 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, 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).

[16] *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).

[17] *Final Designation Order*, 35 FCC Rcd at 6637, para. 9.

[18] *Final Designation Order*, 35 FCC Rcd at 6640, para. 16.

[19] *Final Designation Order*, 35 FCC Rcd at 6638, para. 12.

[20] *Final Designation Order*, 35 FCC Rcd at 6642-43, para. 19.

[21] *Final Designation Order*, 35 FCC Rcd at 6641, para. 22.

[22] *Petition for Reconsideration Filed in PS Docket No. 19-352*, Public Notice, PS Docket No. 19-352, DA 20-831 (PSHSB Aug. 3, 2020).

[23] *See, e.g.*, *Ondas de Vida, Inc., Licensee of FM Translator Station K256BS, Palmdale, California*, DA 20-830 (EB 2020); *Ely Radio, LLC*, Memorandum Opinion and Order, 27 FCC Rcd 7608, 7610, para. 6 (EB 2012). ZTE raises a new argument related to its improved cybersecurity efforts, but this argument did not rise to the level of a material error or omission nor was it unknown to ZTE at the time of this proceeding. Instead, it simply adds more examples to its already argued cybersecurity argument.

A. The Final Designation Order Is Consistent with the Secure Networks Act and Is Within the Bureau's Authority

10. We find that the *Final Designation Order* is consistent with the Secure Networks Act,[24] that the Bureau had delegated authority to adopt that order, and that it was consistent with the *Protecting Against National Security Threats Order*.[25]

11. The Secure Networks Act provides recent evidence and corroboration that Congress and the President continue to see ZTE equipment and services as a national security threat. Specifically, sections 2(b)(1) and 2(c)(3) of the Secure Networks Act provide 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."[26] Indeed, the Secure Networks Act explicitly provides that the Commission is not required to "revisit" actions taken before the Secure Network Act's enactment if such actions are "consistent" with the Secure Networks Act. In other words, the Secure Networks Act explicitly preserves the Commission's existing authority to designate ZTE as a threat to communications networks and the communications supply chain,[27] as we determined in the *Final Designation Order*. We thus continue to find that the Bureau has properly exercised its delegated authority to designate ZTE under the Commission's existing legal authority and as consistent with the Secure Networks Act.

12. We reject ZTE's reading of the 2019 NDAA and Secure Networks Act as limiting our authority to implement a prohibition on USF support for ZTE equipment.[28] ZTE has previously raised this argument and we find no grounds on which to reconsider it here.[29] First, we find that this argument is an untimely and improper petition for reconsideration, essentially seeking to modify the Commission's adoption of section 54.9 in the *Protecting Against National Security Threats Order*.[30] We reject it for that procedural reason alone. Other procedural mechanisms exist to challenge Commission-level decisions, and ZTE declined to pursue those avenues.[31] It cannot attempt to shoehorn those arguments through this petition.

---

[24] *Final Designation Order*, 35 FCC Rcd at 6645, para. 27. ZTE does not dispute the Commission's independent authority to adopt the underlying rule, nor does it raise any significant legal challenges to the *Final Designation Order*.

[25] We note that ZTE does not dispute the Bureau's delegated authority to issue its *Final Designation Order*. We continue to find that the Bureau has authority to issue the *Final Designation Order* pursuant to section 54.9 of the Commission's rules, 47 CFR § 54.9.

[26] *Final Designation Order*, 35 FCC Rcd at 6645-46, para. 27 & n.95 (citing Secure Networks Act § 2(c)(3), which prohibits equipment listed in the 2019 NDAA).

[27] *Final Designation Order*, 35 FCC Rcd at 6636, para. 6.

[28] Petition at 3-4.

[29] Request That the Commission Not Adopt the Initial Designation of ZTE Corporation, WC Docket 18-89, at 4 (Mar. 27, 2020) ("The Act codifies Congress's clear intent that there be no blanket prohibition against the use of USF funds on any and all equipment and services from individual companies, but instead that the prohibition be targeted to equipment and services having the specified capabilities that Congress has identified as being of concern versus those that Congress does not find to be problematic.").

[30] *See* 47 CFR 1.429(d) (establishing a petition for reconsideration deadline of 30 days from public notice of the Commission action). ZTE briefly mentions in its Petition that "Congress and the U.S. Government more broadly have focused their efforts on securing the ICTS supply chain for critical network elements and not on ancillary equipment that is not critical to the network." This, however, is not the forum for reconsidering the scope of the rule as adopted by the Commission in November 2019.

[31] 47 CFR § 1.106(c)-(d); 47 CFR § 1.115, *et al.*

13. Even if we assume *arguendo* that ZTE's argument is not procedurally defective, the argument fails on substantive grounds. We continue to reject the narrow reading advanced by ZTE that the Secure Networks Act requires us to limit the scope of the ZTE 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.[32] Our final designation is governed by section 54.9 of the Commission's rules, which directs the Bureau to decide only whether a company is a national security threat, not which of its equipment should be designated. The Commission's rule itself prohibits the use of USF support to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company that has been so designated. The Bureau does not have the authority to modify the prohibition in section 54.9, which was adopted by the Commission.

14. Because the ZTE Petition does not demonstrate any material error or omission with regard to our findings that we have sufficient legal authority to adopt the *Final Designation Order*, we deny ZTE's Petition.

B. ZTE Does Not Dispute Critical Facts in the Bureau's *Final Designation Order*

15. ZTE's Petition does not dispute critical facts underlying the Bureau's *Final Designation Order* and those uncontroverted facts, standing alone, are enough to sustain the Final Designation of ZTE. As established by the *Protecting Against National Security Threats Order*, a designation is appropriate if the "totality of the evidence" demonstrates an entity (including its subsidiaries, parents, and affiliates) poses a national security threat to communications networks or the communications supply chain.[33] In its *Final Designation Order*, the Bureau made its determination by reviewing the totality of the evidence, which included legal and political analysis from Congress and the Executive Branch, Chinese law experts, as well as evidence of security threats provided by allied intelligence services and outside cybersecurity experts. We also carefully considered and weighed ZTE's previous filings in this proceeding.[34]

16. The Bureau rested its conclusions on the facts laid out by Congress and the Executive Branch, U.S. and allied intelligence agencies, Chinese law experts, security experts, and interested parties (including filings submitted by ZTE). The Bureau also relied on the findings by NTIA, which confirmed the view of the Executive Branch that ZTE poses a threat to the security of communications networks and the communications supply chain.[35] That letter expressed the Executive Branch's full support of the Commission's initial designation of ZTE as a security threat and provided the Executive Branch's analysis of the Chinese National Intelligence Law and Cybersecurity Law, in particular its conclusions that Chinese law imposes both legal and extralegal controls on Chinese citizens and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for the government's intelligence gathering activities.[36] Given the Executive Branch's expertise in both foreign affairs and national security, we gave significant weight to NTIA's conclusions.[37] Importantly, ZTE does

---

[32] *Final Designation Order*, 35 FCC Rcd at 6646, para. 27.

[33] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11438, para. 39.

[34] *Final Designation Order*, 35 FCC Rcd at 6637, para. 9.

[35] *Final Designation Order*, 35 FCC Rcd at 6639, 6641, paras. 14, 17; NTIA Letter at 1. Such concerns have been further buttressed by Sweden's recent decision to disallow ZTE equipment in its networks. *See* Politico**,** *Sweden bans Huawei, ZTE equipment from key parts of 5G network* (Oct. 20, 2020), https://www.politico.eu/article/sweden-bans-huawei-zte-from-key-5g-parts/ (relying on assessments made by the Swedish Armed Forces and the Swedish Security Service to prohibit the use of equipment from Chinese vendors Huawei or ZTE in large parts of their 5G networks).

[36] NTIA Letter at 5.

[37] *Final Designation Order*, 35 FCC Rcd at 6641, para. 17. 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-

(continued….)

not challenge NTIA's interpretation of the Chinese legal regime or the *Final Designation Order*'s reliance on that interpretation.

17. Based on the evidence in the record, we found that ZTE poses a threat to the security of communications networks and the communications supply chain.[38] Specifically, the Bureau determined that either directly though the application of the Chinese National Intelligence Law, or indirectly through the application of political pressure, Chinese companies like ZTE are required to cooperate with intelligence agencies by providing customer information and network traffic information.[39] Article 7 of the Chinese National Intelligence Law "obligates 'all organizations and its 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."[40] The Bureau also determined that Chinese law does not restrain the Chinese government due to its authoritarian nature, lack of sufficient judicial checks, and history of industrial espionage.[41]

18. Additionally, the Bureau found that ZTE has substantial ties to the Chinese government and its military apparatus.[42] ZTE was founded by the Ministry of Aerospace, a Chinese government agency, and it is partly owned by the Chinese government.[43] The composition of ZTE "serves a hybrid of commercial and military needs" with much of the ownership consisting of state-owned enterprises with its own internal Communist Party Committee.[44] We recognized that the composition of ZTE's board has changed in response to a settlement with the Department of Commerce, in which ZTE was also required to pay $1.4 billion for violating a prior settlement agreement with the United States.[45] Regardless, this settlement did not signal assurance in ZTE as a trusted company in the future, and there is still a persistent concern, for the reasons stated by the Bureau in the *Final Designation Order*, that "any director will [and does] have close ties to the Chinese government."[46] And even if ZTE's board has less direct ties to the

(Continued from previous page)
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).

[38] *Final Designation Order*, 35 FCC Rcd at 6638, para. 9*; see Protecting Against National Security Threats Order* 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." *See Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, n.124; *Final Designation Order*, 35 FCC Rcd at 6637, n.34. As the Commission found in the *Protecting Against National Security Threats Order*, we 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 [our] determinations." 47 CFR § 54.9(a); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11440, n.134. This information was contained in classified Appendix E to the *Protecting Against National Security Threats Order*.

[39] *Final Designation Order*, 35 FCC Rcd at 6638, para 12.

[40] China Law Translate, *National Intelligence Law of the P.R.C.(2017)*, available at https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/; *Final Designation Order*, 35 FCC Rcd at 6640, para 17.

[41] *Final Designation Order*, 35 FCC Rcd at 6637, para. 10.

[42] *Id*.

[43] *Final Designation Order*, 35 FCC Rcd at 6639, para. 14.

[44] *Id*.

[45] Secretary Ross Announces $1.4 Billion ZTE Settlement; ZTE Board, Management Changes and Strictest BIS Compliance Requirements Ever, U.S. Department of Commerce (June 7, 2018), https://www.commerce.gov/news/press-releases/2018/06/secretary-ross-announces-14-billion-zte-settlement-zte-board-management.

Chinese government, we noted that it is nevertheless subject to a range of controls that are likely to be exercised by the Chinese government or the Chinese Communist Party.[47]

19. The Bureau also relied upon ZTE's track record of disregarding U.S. laws by violating export control regulations and obstructing investigations.[48] In 2018, ZTE pleaded guilty to violating U.S. sanctions and "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."[49] ZTE also committed hundreds of U.S. sanctions violations related to the shipment of telecommunications equipment.[50]

20. ZTE challenges none of these facts. It does not raise any disagreement with how Chinese law should be interpreted, nor does it challenge our finding that, in practice, the control of China's authoritarian system would effectively prevent ZTE from refusing to follow an espionage demand from the Chinese government.[51] Nor does ZTE dispute that its close ties to the Chinese government make it a particular threat to U.S. national security, as evidenced by U.S. and allied intelligence services' warnings about ZTE. Finally, ZTE does not dispute its history of violating U.S. laws designed to promote U.S. national security and, in fact, engaging in deception to hide its violations of those laws. We find that these facts alone are sufficient to sustain the *Final Designation Order*.

21. Given the totality of the evidence in this proceeding, including unrefuted evidence of ZTE's obligations under Chinese law and as a subject of Chinese political control, the assessments of U.S. and allied intelligence services, the views of Congress and the Executive Branch, as well as our lack of trust in ZTE's supposed compliance efforts, we uphold our decision to designate ZTE as a threat to U.S. communications networks and the communications supply chain.

C. The Totality of the Evidence Demonstrates the Untrustworthiness of ZTE's Systems Regardless of Improved Cybersecurity Programs

22. Although we find that the unrefuted facts of this case are enough to sustain the Bureau's *Final Designation Order*, we continue to find that vulnerabilities and cybersecurity risks plague ZTE equipment. In its *Final Designation Order*, the Bureau found it concerning that ZTE is susceptible to many vulnerabilities and cybersecurity risks.[52] Chinese intelligence agencies have the ability "to tamper with its products in both the design and manufacturing process," which poses a significant threat to our nation's communications networks and supply chain.[53] Even if ZTE has addressed some of these flaws, the Bureau determined that the outstanding risks—coupled with the ability of Chinese intelligence agencies to exploit these risks—outweighed any cybersecurity efforts conducted by ZTE.[54] The Bureau cited several reports in the *Final Designation Order*, which identified vulnerabilities and cybersecurity risks found in ZTE's equipment. These reports also cited concerns that any "technical mitigation techniques" (even sophisticated ones) would be insufficient to protect against Chinese security service

(Continued from previous page)

[46] *Final Designation Order*, 35 FCC Rcd at 6639, para. 14.

[47] *Id*.

[48] *Final Designation Order*, 35 FCC Rcd at 6642, para. 19.

[49] *Id.*

[50] *Id.*

[51] See *Final Designation Order*, 35 FCC Rcd at 6637, para. 10 ("The [*Protecting Against National Security Threats 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.'").

[52] *Final Designation Order*, 35 FCC Rcd at 6643, para. 22.

[53] *Final Designation Order*, 35 FCC Rcd at 6638, para 13.

[54] *Final Designation Order*, 35 FCC Rcd at 6644, para. 24.

exploitation, and ZTE's citation of additional and improved techniques does not alleviate the concern.[55] As a result, the Bureau was concerned with the trustworthiness and security of ZTE's equipment when it evaluated the totality of evidence in making this final determination.

23. The Bureau properly rejected ZTE's past assertions about its compliance and security programs. However, ZTE raises new arguments that were not previously introduced in this proceeding regarding its cybersecurity efforts.[56] Specifically, ZTE discusses how it improved its end-to-end security assurance in its products and services and published this in their ZTE Cybersecurity White Paper.[57] In this White Paper, ZTE goes on to describe how it has received certifications from independent parties; focused on industry engagement; focused on its participation in standards organizations; and increased collaboration on handset security.[58] We reject these new arguments made by ZTE regarding its cybersecurity efforts.[59]

24. These new arguments do not persuade us to change our findings in light of the totality of the evidence in this proceeding. While ZTE's White Paper appears to showcase an effort to improve its security practices, we find that, notwithstanding these efforts, there is substantial evidence in the record that flaws and vulnerabilities continue to exist.[60] Even the most sophisticated mitigation techniques do not provide sufficient protection against Chinese security service exploitation.[61] As we found in the *Final Designation Order*, manufacturers can show they have remedied discrete security vulnerabilities, but it does not change the fact that ZTE, as a whole, is an untrustworthy vendor for purposes of securing our communications networks and communications supply chain.[62] Additionally, given ZTE's track record of persistent vulnerabilities in its systems,[63] we must consider the likelihood that its products still contain unknown vulnerabilities, even if it has attempted to resolve known vulnerabilities. This risk is magnified by the ability of the Chinese government to require ZTE to abide by its national intelligence laws.[64]

25. Additionally, ZTE's efforts to reduce cybersecurity risk and vulnerabilities from third parties do not eliminate the threats from its close ties to the Chinese government and its legal obligation under Chinese law. ZTE does not dispute our analysis of its obligations under Chinese law. It is especially alarming considering the Bureau and Commission found that Chinese intelligence agencies have opportunities to tamper with its products in both the design and manufacturing processes.[65] As cited

[55] *Final Designation Order*, 35 FCC Rcd at 6643, para. 22.

[56] ZTE specifically argues that the Bureau should consider "all available evidence in its cybersecurity efforts since 2018 in order to make an informed decision about whether ZTE poses a security threat." Specifically, ZTE mentions that in past filings, it has discussed how it improved its cybersecurity efforts by launching three global Cybersecurity labs in 2019. ZTE additionally criticizes the reports that we cited in our *Final Designation Order*.[56]

[57] Petition at 14, Exhibit B. The ZTE Cybersecurity White Paper was published by ZTE on March 2019 and focuses on discussing the security implications implemented in its products. The research and opinions in this Paper were directly provided by ZTE. The Paper outlined the company's cybersecurity strategy and its end-to-end cybersecurity practices, for example, its practices with respect to R&D Security, Supply Chain Security, Personal Data Protection and Independent Security Assessment.

[58] Petition at 15-19.

[59] As an initial matter, we procedurally dismiss any new arguments not raised accordingly by ZTE under 47 CFR § 1.106(c). Notwithstanding the procedural bar to these arguments, they also fail on substantive grounds.

[60] *See Final Designation Order*, 35 FCC Rcd at 6643, para. 22 (citing *Protecting Against National Security Threats Order,* 34 FCC Rcd at 11448, para. 61).

[61] *Final Designation Order*, 35 FCC Rcd at 6643, para. 22.

[62] *Final Designation Order*, 35 FCC Rcd at 6644, para. 24.

[63] *See Final Designation Order*, 35 FCC Rcd at 6643-44, para. 22-23.

[64] *See Final Designation Order*, 35 FCC Rcd at 6644, para. 24.

in the *Protecting Against National Security Threats Order*, the Department of Homeland Security Science & Technology Directorate's report noted how these vulnerabilities are built into the phones during the manufacturing process and can allow for access to user data.[66] Implementing standards or obtaining certifications from third parties do not account for intrusions that may be mandated by the Chinese government.[67] Reviews and certifications from standards organizations are not evidence that ZTE will disregard the Chinese government's national security mandates.

26. Ultimately, the Bureau cited the reports to highlight the cybersecurity risks and vulnerabilities that ZTE poses to our communications networks and services.[68] We find ZTE's arguments about its cybersecurity programs to be unpersuasive as ZTE fails to refute the actual risks and vulnerabilities discovered in its equipment. Further, ZTE does not refute our finding in the *Final Designation Order* that its mitigation techniques would be insufficient to protect against Chinese security service exploitation.[69] Finally, ZTE's claims fail to negate the fact that the company would have to abide by Chinese law, which requires ZTE to assist the Chinese government with espionage activities. We therefore uphold the *Final Designation Order*'s findings.

D. ZTE's Recent Compliance Efforts Do Not Outweigh Other Evidence

27. The *Final Designation Order* also took into account ZTE's record of knowingly violating U.S. law, obstructing U.S. investigations, and making false statements to U.S. authorities even after entering a guilty plea for violating U.S. trade sanctions.[70] While ZTE argues it had taken steps toward compliance, we do not find these efforts sufficient to reconsider our decision to designate it as a national security threat. Given ZTE's demonstrated willingness to flout U.S. national security laws, and its past dishonesty in attempting to cover up such violations, we find its assertions about its compliance programs to be unavailing.

28. In its Petition, ZTE emphasizes its commitment to compliance as part of its company's core values.[71] ZTE describes a number of efforts to enhance its compliance regime.[72] These efforts do not persuade us to change our decision when we consider such efforts in light of the totality of evidence. As we made clear in the *Final Designation Order*, "ZTE's claims of improved compliance [] do not deserve significant weight in our consideration of the totality of the evidence."[73] ZTE's compliance efforts do not change the fact that ZTE has a track record of breaking U.S. law and attempting to cover up such violations after the fact.[74] In the *Protecting Against National Security Threats Order*, the Commission noted that "ZTE pleaded guilty to violating our embargo on Iran by sending approximately $32 million dollars' worth of U.S. goods to Iran and obstructing justice in an effort to thwart DoJ's

(Continued from previous page)

[65] *Final Designation Order*, 35 FCC Rcd at 6638, para. 13.

[66] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11488, para. 61.

[67] *See Final Designation Order*, 35 FCC Rcd at 6643, para. 22.

[68] In its Petition, ZTE argues against the reports by noting that its market is focused on consumer devices. But, this would not be pertinent for purposes of this rule considering USF does not fund end-user devices. *See Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, para. 28.

[69] *Final Designation Order*, 35 FCC Rcd at 6643, para 22.

[70] *Final Designation Order*, 35 FCC Rcd at 6642, para. 19.

[71] Petition at 20.

[72] Petition at 20.

[73] *Final Designation Order*, 35 FCC Rcd at 6643, para. 21.

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

investigation."[75] In the *Final Designation Order*, we relied on the fact that ZTE had violated export laws and trade agreements, as well as obstructed U.S. investigations, which indicated a clear disregard for U.S. law and national security.[76] These actions evince a company culture in which lying and covering up violations of U.S. national security laws are endemic. The actions ZTE described in its Petition are steps towards complying with minimum industry standards, but they do not convince us of ZTE's complete honesty with its business actions moving forward, nor do they remove ZTE's obligation to abide by the Chinese government's national security requirements, which poses an inherent risk to our communications equipment and services.

IV. ORDERING CLAUSES

29. Accordingly, **IT IS ORDERED**, pursuant to sections 1, 4(i), 4(j), 5(c), 214, 229, 254, and 405 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, 405, 1004, and section 1.106 of the Commission's rules, 47 CFR § 1.106, that this order **IS ADOPTED**.

30. Accordingly, IT **IS ORDERED** that, pursuant to section 1.106 of the Commission's rules, the Petition for Reconsideration filed by ZTE is hereby **DENIED.**

31. **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

Lisa M. Fowlkes
Chief
Public Safety and Homeland Security Bureau

[75] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11149, para. 62.

[76] *Final Designation Order*, 35 FCC Rcd at 6642, para. 20.