ZTE中兴

3 February 2020

By Electronic Mail

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	)	WC Docket No. 18-89
	)	
	)	
ZTE Designation	)	PS Docket No. 19-352
	)	

REQUEST THAT THE COMMISSION NOT ADOPT THE INITIAL DESIGNATION OF ZTE CORPORATION

ZTE Corporation ("ZTE" or the "Company")[1] hereby submits this filing in the above-captioned proceeding to request the Federal Communications Commission ("Commission") not to adopt the initial determination that ZTE is a "covered company" under Section 54.9 of the Commission's rules.[2] ZTE respects the Commission must take steps it believes are necessary to address U.S. national security concerns and to protect the telecommunications security of the United States. We respectfully request, however, that the Commission take the additional time afforded by the Commission's process for reviewing comments in response to initial designations in order to consider additional information that may be helpful to the Commission in reaching a

[1] ZTE Corporation is a publicly-traded corporation and was founded in 1985 and is a global leader in telecommunications and information technology.

[2] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation*, WC Docket No. 18-89, PS Docket Nos. 19-351, 19-253, Report and Order, Further Notice of Proposed Rulemaking, and Order, FCC 19-121 (2019) ("Initial Designation Order"); *see also 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 2014 (PSHSB rel. Jan. 3, 2020); 47 C.F.R. § 54.9.

final determination.[3] In particular, we believe it would be useful for the Commission to understand the progress ZTE has made in two important areas: (1) compliance with U.S. export controls and economic sanctions; and (2) cybersecurity assurance in ZTE's products and services. We believe that this progress is material to the Commission's final determination in this matter and provide some key points on these topics here for the Commission's benefit and understanding.

With respect to the first area, ZTE has settled its case relating to export control and sanctions violations --- ZTE Corporation is not listed by the U.S. Departments of Commerce or Treasury for any export control or sanctions restrictions targeting it. ZTE's senior leadership is committed to ensuring that our Company conducts business only in compliance with all applicable laws where we are operating, including U.S. export and sanctions laws and regulations. ZTE has spent hundreds of millions of dollars to implement a compliance program relating to U.S. export control compliance regulations and continues to work to enhance its compliance program. As part of this work, ZTE has implemented an updated global export control compliance program that applies to all corporate levels of ZTE, its subsidiaries, affiliates, and other entities worldwide over which ZTE has majority ownership or control. ZTE has adopted export compliance practices with a focus on People, Process, Technology and Industry Outreach.

- **People**. From top to working level, ZTE is committed to export compliance. Senior management supports export compliance policies and procedures and provides resources for compliance in terms of human resources and funding. The Export Control Compliance Committee under ZTE Board oversees compliance with export control and economic sanctions laws, and the Compliance Management Committee organizes the compliance management system and makes decisions on compliance matters. ZTE has created an

[3] 47 C.F.R. § 54.9(b)(2) (providing that, if any opposition to an initial designation is received, the Commission will reach a final determination as to whether the company that is the subject of the opposition should be designated as a covered company within 120 days of the initial designation); Initial Designation Order at para. 40.

Export Compliance Team with over 60 headcounts and more than 100 other Compliance Functions headcounts. Employees companywide continue to participate in and support export control compliance training. The Company is committed to fostering a strong compliance culture. This commitment starts with senior management and employees and continuous training.

- **Process**. The Company is in the process of building a best-in-class export control compliance program ("ECP") and consistent with the Company's business practices, this goal is a ZTE target and principle. The Company continues to improve its ECP to ensure export control compliance policies and procedures are fully implemented, prevent systemic risks, and safeguard the interests of ZTE and its business partners, under the premise that export compliance is an essential requirement for ZTE employees, contractors and businesses.
- **Technology.** Recognizing the importance of technology and automation in a global compliance program ZTE has implemented SAP Global Trade Systems ("GTS") software in certain of its businesses. ZTE has also developed and been deploying certain innovative screening solutions such as robotic screening tools to support transactional and ad hoc screening.
- **Industry Outreach**. In order to communicate and promote export control compliance awareness ZTE continues to conduct industry outreach through Symposia, Compliance Associations, and other communications with business partners. ZTE is a member of The National Compliance Committee of the China Council for the Promotion of International Trade ("CCPIT"), which is a working mechanism for promoting the development of enterprise compliance. ZTE also participated in several Compliance Forums in China

and presented at several conferences in China. ZTE hosted the ZTE Multinational Enterprise Trade Compliance Forum in Shenzhen in November 2019. Guests from ZTE, industry associations, industry-renowned law firms, and multinational companies, including prominent U.S. companies, were invited to discuss and exchange views on export compliance, including topics such as the compliance management commitment in the global trade operations of multinational enterprises and mitigating export control risks.

With respect to the second area, ZTE continues to make progress to address cybersecurity. Providing secure and trustworthy products and services for our customers is one of ZTE's highest priorities. Our vision and motto on cybersecurity is "Security in DNA, Trust through Transparency." Toward that end, ZTE has adopted industry standards and best practices to develop cybersecurity governance with three central pillars: People, Process, and Technology.

- **People**. ZTE created a Cybersecurity Committee, chaired by our senior management. This Committee is responsible for deploying cybersecurity assurance across the management level in our Supply Chain, R&D, and Engineering Services business units. Leveraging industry best practices, ZTE has built a governance structure with three lines of defense: (1) The first line implements security throughout the entire company – we have dedicated 1500 specialists in all business units; (2) The second line verifies security, which is performed by our Product Security Department, consisting of 70 employees; and (3) The third line audits security, which is performed by ZTE's Audit Department and external third party auditors. ZTE's Chief Security Officer is empowered to veto or delay the release of any product for noncompliance with ZTE's cybersecurity standards.
- **Process**. With industry standards and best practices as our benchmark, ZTE is embedding security controls into the full product life cycle (e.g., evaluating the maturity level in R&D

referring to BSIMM,[4] evaluating supply chain and engineering processes against NIST Cybersecurity Framework to check if security is by design and by default).

- **Technology**. ZTE is committed to ensuring that our products conform to industry standards, including 3GPP, ITU, SEI CERT secure coding standards, among others. ZTE's end-to-end solution integrates security features by design. ZTE uses security tools and methods, including Nessus, AppScan, WebInspect and AWVS for black box testing, Coverity, Klockwork and Fortify for source code review, Defensics for fuzzing testing, MetaSploit and Burp Suite for penetration testing.

Consistent with our commitment to cybersecurity governance and in an effort to move towards even greater transparency and collaboration, ZTE launched three Cybersecurity Labs globally in 2019. These labs allow our customers, regulators and other interested third parties to perform independent security assessment and audits on our products, services and processes.

Again and importantly, ZTE respects that the Commission must take whatever steps it believes are appropriate to protect U.S. national security and the security of U.S. telecommunications. ZTE believes that it is appropriate to ask the Commission to take additional time to assess ZTE's enhancements in the area of U.S. export control and economic sanctions compliance and security controls in ZTE products. If, upon consideration of this information, the Commission is of the view that it needs more information from ZTE, we would welcome the opportunity to present it to the Commission on a going forward basis.

ZTE's management is working to ensure that ZTE is a model company in both areas and hopes that its efforts will be the basis for future cooperation. ZTE would welcome the opportunity to meet with the Commission, listen to, and try to address any concerns that it might have.

---

[4] The Building Security In Maturity Model ("BSIMM") is a study of existing software security initiatives.

Respectfully submitted,

_____

[Shen Nan]
[Senior Vice President, Chief Legal Officer]

ZTE Corporation
5/F, Building A, Hi-tech Road South,
Hi-tech Industrial Park Nanshan District,
Shenzhen, P.R.China, 518057

February 3, 2020