ZTE

ZTE (USA) Inc.

2425 N. Central Expressway Suite 323 • Richardson TX 75080 • (972) 671-8885 • Fax: (972) 331-8094

March 23, 2020

Submitted Electronically: www.regulations.gov

Office of Federal Financial Management
Office of Management and Budget
Executive Office of the President
725 17th Street, NW
Washington, DC 20500

RE: Comments on Proposed Guidance for Grants and Agreements, [200.216], Docket Number 2019-OMB-0005

To Office of Federal Financial Management:

On behalf of ZTE USA, Inc. ("ZTE"), which is headquartered in Richardson, Texas, we are writing to provide comments on Docket Number 2019-OMB-0005, Proposed Guidance for Grants and Agreements ("Proposed Guidance"). ZTE's objective is to serve an important and underserved consumer segment in the United States by providing affordable consumer devices that are secure and trustworthy. Importantly and as an initial matter, ZTE respects the U.S. Government in protecting its national security, and we appreciate the opportunity to provide input on the possible impact of proposed additions to 2 CFR 200.216, "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment."

ZTE's comments here are focused on two points: 1) whether the Proposed Guidance is consistent with the scope of the legislation passed by Congress and 2) ensuring that Office of Federal Financial Management ("OFFM") considers the significant steps that ZTE has taken to comply with U.S. law and global security best practices.

As you know, effective August 13, 2020, Section 889(b)(1) of the National Defense Authorization Act of 2019 ("NDAA") prohibits executive branch agencies from "obligat[ing] or expend[ing] 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 the equipment, services, or systems described in subsection (a)." In turn, NDAA Section 889(a) defines the universe of covered equipment and services to include "covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." NDAA Section 889(f)(3)(A) explains that the term "covered telecommunications equipment or services" applies to, among other things, "equipment produced by … ZTE Corporation

(or any subsidiary or affiliate of [ZTE])." Thus, ZTE USA is directly affected by the Proposed Guidance, as are our U.S. customers and suppliers.

As written, the statute prohibits all federal agencies from (1) expending, or (2) entering into a contract to expend, federal loan or grant funds to procure or obtain "covered telecommunications products or services." However, the Proposed Guidance, if ultimately adopted, would impose a much broader restriction than the one contained in Section 889(b)(1), with a significant retroactive effect that is not found in the statute. The Proposed Guidance calls for a prohibition on the expenditure of federal funds by grant, cooperative agreement, or loan recipients from contracting with entities that merely "use covered technology." In particular, the Proposed Guidance states: "Grant, cooperative agreement, and loan recipients are prohibited from using government funds to enter into contracts (or extend or renew contracts) with entities that ***use*** covered technology."[1] The Proposed Guidance further states that "[t]his prohibition applies even if the contract is not intended to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services."

In view of this language, we are concerned that, if the OFFM were to finalize the Proposed Guidance as written, all federal agencies would adopt regulations that exceed the scope of NDAA Section 889(b)(1). Simply put, a prohibition on the use of federal funds to enter into contracts to purchase "covered telecommunications equipment or services" is altogether different from a prohibition on entering into contracts with parties that "use covered technologies."

We respectfully submit that the language of Section 889(b) is clear and as such it cannot be expanded beyond its plain meaning.[2] As the U.S. Supreme Court has explained, "If the intent of Congress is clear, that is the end of the matter; for [a] court, as well as [an administering] agency, must give effect to the unambiguously expressed intent of Congress."[3] A regulatory agency can fill a gap in statutory meaning if "the statute is ambiguous."[4] However, an interpretation at odds with the plain meaning of a statute is not permissible.[5]

If OFFM were to adopt the Proposed Guidance, it could adversely affect a much broader group of U.S. businesses, non-profit organizations, universities, and other parties than Congress intended. Section 889(b)(1) is a prospective provision that Congress meant to ban the expenditure of federal grant and loan funds for **future purchases** of covered technologies. However, if the Proposed Guidance is implemented in its current form, these federal funds could not be expended in contracts with parties who **previously**

---

[1] Emphasis added.

[2] *Wisconsin Cent. Ltd. v. United States*, 138 S. Ct. 2067, 2070 (2018).

[3] *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 842-843 (1984).

[4] *Encino Motorcars, LLC v. Navarro*, 136 S. Ct. 2117, 2124 (2016).

[5] *Pereira v. Sessions*, 138 S. Ct. 2105, 2113 (2018) (quoting *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. at 842-843).

purchased and continue to use covered equipment. In this way, OFFM would make Section 889(b)(1) apply retroactively to parties that acquired "covered equipment" **in the past**. Such a burden would be especially onerous for affected parties already involved in ongoing grants, cooperative agreements, or loans that require future payments or are pending extension or renewal.

The Proposed Guidance contains no analysis of the potential impact on grant, cooperative agreement, and loan recipients and their U.S. contractors, subcontractors, vendors, and suppliers. Federal grant, cooperative agreement, and loan recipients would have to undergo an onerous, burdensome, and difficult examination of whether any of their contractors, subcontractors, vendors, or suppliers use ZTE equipment – no matter how remote such use might be from the federal grant, cooperative agreement, or loan at issue or how *de minimis* such use might be. Affected parties would have to forego important business opportunities or remove any such equipment, which could entail major costs and disruptions.

We also note two additional issues. First, the Proposed Guidance would extend the proposed restriction to "cooperative agreements," which are not mentioned in the statute; Section 889(b)(1) refers only to "loan or grant funds." Second, the Proposed Guidance does not define either of the terms "critical technologies" or "substantial or essential component." As you are likely aware, in implementing Section 889(a)(1)(A) related to federal procurement, definitions were included for these terms. Given the substantial overlap of entities receiving both federal contracts and grants, consistent definitions should be included in both regulations.

Separately, as OFFM may be aware, our parent company, ZTE Corporation, has committed to ensuring it conducts business in compliance with all applicable laws, including U.S. export and sanctions laws and regulations and has implemented an updated global export control compliance program that applies to all corporate levels of ZTE, its subsidiaries, affiliates, and other entities worldwide.

With regard to cybersecurity, ZTE Corporation has adopted global industry standards and best practices to develop cybersecurity governance with three central pillars: people, process, and technology. ZTE Corporation created a Cybersecurity Committee, chaired by global senior management and responsible for deploying cybersecurity assurance across the Supply Chain, research and development ("R&D"), and Engineering Services. Cybersecurity is a top company priority throughout the full product life cycle, and ZTE Corporation collaborates extensively with U.S. suppliers, partners, and customers on the security of anything ZTE provides to the U.S. market.

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

Furthermore, as recently as February 18, 2020, President Trump announced that:

> The United States cannot, [and] will not, become such a difficult place to deal with in terms of foreign countries buying our product, including for the always used National Security excuse, that our companies will be forced to leave in order to remain competitive....I have seen some of the regulations being circulated, including those being contemplated by Congress, and they are ridiculous. I want to make it EASY to do business with the United States, not difficult. Everyone in my Administration is being so instructed, with no excuses.[6]

ZTE hopes that OFFM takes from this letter the seriousness with which ZTE is approaching compliance with applicable laws and fulfillment of its compliance commitment. Like many large multinational corporations, ZTE endeavors to comply with applicable law in all of the countries in which it does business. In particular, ZTE is fully committed to complying with all applicable laws and regulations in the United States and to continuing to serve the U.S. market.

Thank you for the opportunity to provide these comments. We would be happy to meet with you or provide additional information that may be useful as you consider finalizing the proposed guidance.

Sincerely,

/s/

Angela Simpson
Vice President, U.S. Government Affairs

[6] President Donald Trump, Twitter Post, February 18, 2020, https://twitter.com/realDonaldTrump/status/1229790099866603521.