STEVE CHABOT, OHIO
CHAIRMAN

NYDIA M. VELAZQUEZ, NEW YORK
RANKING MEMBER

Congress of the United States

U.S. House of Representatives

Committee on Small Business

2361 Rayburn House Office Building
Washington, DC 20515-6315

Memorandum

To: Members, Committee on Small Business
From: Committee Staff
Date: June 25, 2018
Re: Hearing: "ZTE: A Threat to America's Small Businesses"

On Wednesday, June 27, 2018 at 11:00 a.m. in Room 2360 of the Rayburn House Office Building, the Committee on Small Business will hold a hearing to examine the imminent threat posed to America's small businesses by the Chinese telecommunications firm Zhongxing Telecommunications Equipment Corporation (ZTE). The hearing will provide Committee Members the opportunity to hear from national security experts and representatives of cybersecurity firms on steps the Administration can take to protect small businesses and American citizens from the dangers presented by ZTE. The hearing will also investigate ongoing efforts by both the public and private sectors to reduce the challenges small businesses face in dealing with illicit Chinese-backed enterprises.

I. Background

As small businesses increasingly rely on foreign technology products and services, they become even more susceptible to cyber attacks. Many small business owners are underequipped to protect themselves from basic cyber attacks and face significant hurdles in guarding against sophisticated foreign state-backed cyber actors. As the Committee has learned in past hearings,[1] some foreign-backed firms have taken steps to expose small businesses' information technology systems as a means of infiltrating America's critical infrastructure and weakening our national security. Foreign governments – through subversive tactics – can employ state-backed firms to orchestrate cyber attacks, cyber espionage, and other national strategic objectives, making it difficult to identify the responsible entity. Additionally, the Small Business Committee has learned through hearings that some foreign-backed firms have reassessed their strategies to expose weaknesses in the United States' information technology infrastructure. Small businesses are at additional risk for these cyber threats because they generally have less capital to purchase security hardware and software, fewer staff members to monitor their systems, and less time to develop cybersecurity defense strategies.

As a global leader in producing intellectual property, America's private and public institutions will continue to be primary targets for cyber criminals. The Internet Crime

[1] *Foreign Cyber Threats: Small Business, Big Target*, U.S. HOUSE SMALL BUS. COMM. (Jul. 6, 2016), https://smallbusiness.house.gov/calendar/eventsingle.aspx?EventID=399199.

Complaint Center within the United States Department of Justice recorded 298,728 cybersecurity-related complaints in its 2016 report.[2] There have been steady increases year over year since the year 2000 (3,762,348 total reported complaints). Some of the key targets include the nation's critical infrastructure, federal and state governments, and private businesses. Moreover, the expansion of global communications technology leaves United States businesses exceptionally vulnerable to cyber threats associated with integrated dependencies, particularly those resulting from foreign-sourced telecommunications supply chains used for national security applications.[3]

The Government Accountability Office (GAO) notes in a 2012 report that the Federal Bureau of Investigation (FBI) has determined that foreign state actors pose a serious cyber threat to the telecommunications supply chain.[4] It is also clear that many foreign nations are responsible for direct cyber attacks on the United States in an effort to gain intellectual property and economic information. The Office of the National Counter Intelligence Executive released a report on October 11, 2011 stating that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each year from computer systems in the federal government, corporations, and academic institutions. They identified China and Russia as the two largest participants in cyber espionage.[5]

In a 2012 report by the House Permanent Select Committee on Intelligence, United States businesses and cyber security experts reported persistent network disturbances that were traced back to China and were thought to be supported by the Chinese government.[6] The same report noted that some services and private companies display their cyber capabilities through a supply of telecommunications components and systems marketed directly to United States businesses and entities.[7] Furthermore, a Department of Defense (DOD) study states that when safeguarding against and assessing threats posed by nation-state actors "means and opportunity are present throughout the supply chain and lifecycle of software development."[8] This is particularly troublesome for small businesses that not only rely on products from, but also engage in commerce with, globalized telecommunications firms from countries like China.

---

[2] INTERNET CRIME COMPLAINT CENTER, 2016 INTERNET CRIME REPORT 14 (2016), *available at* https://pdf.ic3.gov/2016_IC3Report.pdf

[3] PERMANENT SELECT COMMITTEE ON INTELLIGENCE, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE 1 (2012), [hereinafter "Intelligence Committee Report"], *available at* https://intelligence.house.gov/press-release/investigative-report-us-national-security-issues-posed-chinese-telecommunications.

[4] GOVERNMENT ACCOUNTABILITY OFFICE (GAO), IT SUPPLY CHAIN, NATIONAL SECURITY RELATED AGENCIES NEED TO BETTER ADDRESS RISKS 11 (2012) (GAO-12-361), *available at* http://www.gao.gov/assets/590/589568.pdf.

[5] OFFICE OF NATIONAL COUNTER INTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 4 (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[6] Intelligence Committee Report.

[7] *Id*. at 2, 3.

[8] DOD, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON MISSION IMPACT OF FOREIGN INFLUENCE ON DOD SOFTWARE VIII (2007), *available at* http://www.acq.osd.mil/dsb/reports/ADA486949.pdf.

II. Background on the ZTE Case

Vulnerabilities in the information technology supply chain are especially at risk because foreign telecommunications firms are capable of exploiting these weaknesses to carry out criminal activities. In documents made public by the Bureau of Industry and Security (BIS),[9] China-based ZTE Corporation outlines the risks associated with doing business in sanctioned countries and provides a model, as well as advocates for the use of shell companies to subvert United States export control laws. In fact, the document states explicitly that "[t]he biggest advantage of [this model] is that it is more effective, [because it's] harder for the U.S. Government to trace it or investigate the real flow of the controlled commodities."[10] The document also notes that "once our company violates the relevant U.S. export control provisions, [the U.S. Government] might carry out civil and criminal punishments against U.S. suppliers, which will lead to increased difficulty for our company to obtain the relevant U.S. technologies and components later."[11] ZTE's smartphones use Qualcomm microchips and Corning glass, and U.S. companies provide an estimated 25 to 30 percent of the components used in ZTE's products.[12] Many of the American companies that provide component parts to ZTE are small businesses.

In July 2012, the FBI determined that ZTE had sold banned technology to Iran and used the methods outlined above to mask its transaction history in an effort to undermine the Department of Commerce's investigations into its sanctions violations.[13] In the spring of 2016, Reuters reported that Commerce was moving to impose export restrictions on ZTE for its violations. Subsequently, public trading of ZTE shares was immediately halted in Hong Kong and Shenzhen which encouraged ZTE to cooperate with BIS and replace its President and Chairman of the Board, Shi Lirong.[14]

On June 28, 2016, BIS extended the temporary general license[15] (TGL) which removed the export restrictions that had been imposed earlier in 2016 on ZTE and its affiliate, ZTE Kangxun Telecommunications Ltd. The TGL was originally issued on March 24, 2016 and effective until June 30, 2016. The final rule issued by BIS extended the TGL until August 30, 2016, but ZTE remained on BIS's Entity List.[16] On November 18, 2016, BIS announced another extension of its TGL for exports, reexports, and in-country transfers to ZTE until February 27,

---

[9] https://bis.doc.gov/index.php/documents/update-2017/2156-zte-the-investigation-settlement-and-lessons-learned-recap/file.
[10] https://www.bis.doc.gov/index.php/forms-documents/doc_download/1436-proposal-for-english.
[11] *Id*.
[12] *Id*.
[13] Intelligence Committee Report, *supra* note 1.
[14] https://www.bloomberg.com/news/articles/2016-03-07/china-s-zte-halted-from-trade-after-report-of-u-s-export-curbs.
[15] 82 Fed. Reg. 11,505 (Feb. 24, 2017) [hereinafter "February Extension"], *available at* https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2017/1647-82-fr-11505-tgl-extension-of-validity-final-rule-2-24-17/file.
[16] https://www.cooley.com/news/insight/2016/2016-06-28-us-extends-temporary-license-for-exports-to-chinese-telecom-company-zte.

2017.[17] Finally, after ZTE appointed nine new board members, ZTE was granted a fifth reprieve. The U.S. government's TGL issuance stretched to March 29, 2017.[18]

On March 23, 2017, ZTE reached an agreement for a combined penalty and forfeiture of $1.19 billion. The Department of Justice stated that "ZTE Corporation has agreed to enter a guilty plea and to pay a $430,488,798 penalty to the U.S. for conspiring to violate the International Emergency Economic Powers Act by illegally shipping U.S.-origin items to Iran, obstructing justice and making a material false statement. ZTE simultaneously reached settlement agreements with Commerce's BIS and the U.S. Department of the Treasury's Office of Foreign Assets Control. In total, ZTE has agreed to pay the U.S. government $892,360,064. The BIS has suspended an additional $300,000,000, which ZTE will pay if it violates its settlement agreement with the BIS."[19]

III. Additional ZTE Violations and Penalties

ZTE was required to complete and submit audit reports regarding compliance and make truthful disclosures of requested information.[20] The plea agreement also prohibited ZTE from continuing to make false or misleading statements to the government.[21] "Subsequently, BIS requested a status report from ZTE regarding certain named individuals who ZTE reported had been subjected to harsh discipline as an indication of ZTE's commitment to compliance."[22] BIS found that ZTE was again in violation of the agreement for falsifying reports. Not only had some of the named individuals not been disciplined, but many ZTE employees received bonuses.[23] Worse still, ZTE admitted to BIS that it had falsified correspondence with BIS.[24]

As a result, on March 13, 2018, BIS notified ZTE that Commerce would be activating the conditionally suspended sanctions based on ZTE's false statements.[25] Ultimately, BIS determined that ZTE had continued to make false statements to the United States government and activated the suspended denial order to ZTE.[26]

The order issued by BIS on April 15, 2018 prohibits ZTE from "directly or indirectly, participat[ing] in any way in any transaction involving any commodity, software or technology

---

[17] https://www.steptoeinternationalcomplianceblog.com/2016/11/bis-again-extends-zte-temporary-general-license/.
[18] February Extension, *supra* note 15.
[19] DEPT. OF JUSTICE., *ZTE Corporation Agreement*, https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending (last visited Jun. 25, 2018).
[20] United States of America v. ZTE Corporation, No. 3-17CR0120K *available at* https://www.justice.gov/opa/press-release/file/946276/download.
[21] *Id.*
[22] https://www.bakerlaw.com/alerts/bis-activates-export-denial-against-chinese-telecom-titan-zte.
[23] *Id.*
[24] *Id.*
[25] In the Matter of: Zhongxing Telecommunications Equipment Corporation ZTE Plaza, Keji Road South Hi-Tech Industrial Park Nanshan District, Shenzhen China; ZTE Kangxun Telecommunications Ltd. 2/3 Floor, Suite A, Zte Communication Mansion Keji (S) Road Hi-New Shenzhen, 518057 China Respondent'; Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and Zte Kangxun Telecommunications Ltd., 83 Fed. Reg. 17644 (April 23, 2018).
[26] *Id.*

. . . exported or to be exported from the United States."[27] The order effectively shut down ZTE operations in the United States.

The Order prohibited any individual directly or indirectly, from the following:

A. Export or reexport to or on behalf of a Denied Person any item subject to the Regulations;

B. Take any action that facilitates the acquisition or attempted acquisition by a Denied Person of the ownership, possession, or control of any item subject to the Regulations that has been or will be exported from the United States, including financing or other support activities related to a transaction whereby a Denied Person acquires or attempts to acquire such ownership, possession, or control;

C. Take any action to acquire from or to facilitate the acquisition or attempted acquisition from a Denied Person of any item subject to the Regulations that has been exported from the United States;

D. Obtain from a Denied Person in the United States any item subject to the Regulations with knowledge or reason to know that the item will be, or is intended to be, exported from the United States; or

E. Engage in any transaction to service any item subject to the Regulations that has been or will be exported from the United States and which is owned, possessed or controlled by a Denied Person, or service any item, of whatever origin, that is owned, possessed or controlled by a Denied Person if such service involves the use of any item subject to the Regulations that has been or will be exported from the United States. For purposes of this paragraph, servicing means installation, maintenance, repair, modification or testing.[28]

IV. ZTE Settlement

On June 7, 2018, Secretary of Commerce Wilbur Ross announced that ZTE agreed to additional penalties and compliance measures to replace BIS's April denial order.[29] As a result of the settlement, ZTE agreed to pay $1 billion and place an additional $400 million in suspended penalty money in escrow before BIS will remove ZTE from the Denied Persons List.[3031] These

[27] *Id*.
[28] *Id*.
[29] https://www.commerce.gov/news/press-releases/2018/06/secretary-ross-announces-14-billion-zte-settlement-zte-board-management.
[30] The Denied Persons List is a list of people and companies whose export privileges have been denied by the Department of Commerce's Bureau of Industry and Security (BIS). An American company or individual may not participate in an export transaction with an individual or company on the Denied Persons List. https://www.law.cornell.edu/wex/denied_persons_list.
[31] https://www.commerce.gov/news/press-releases/2018/06/secretary-ross-announces-14-billion-zte-settlement-zte-board-management.

penalties are in addition to the $892 million in penalties ZTE has already paid to the United States government under the March 2017 settlement agreement.[32]

Commerce also stated that ZTE will be required to "retain a team of special compliance coordinators selected by and answerable to BIS for a period of 10 years."[33] The imbedded team will be tasked with monitoring ZTE's compliance with U.S. export control laws.[34] ZTE will also be required to replace the entire board of directors and senior leadership for both ZTE entities.[35]

Lastly, Commerce announced that the new agreement imposes an additional denial order that is suspended for 10 years, which BIS can activate in the event of additional violations during the ten-year probationary period. Secretary Ross stated that "BIS is imposing the largest penalty it has ever levied and requiring that ZTE adopt unprecedented compliance measures."[36]

V. Policy Initiatives for the 115th Congress

There is strong bipartisan commitment from both chambers of Congress to not only hold ZTE accountable for the crimes that it has committed, but also to protect the national security of Americans and American small businesses. Legislative action has been taken in response to the Department of Commerce's announcement that it has reached an agreement with ZTE.

On June 11, 2018, Senator Tom Cotton's (R-Arkansas) Amendment 2514 was included in the FY2019 National Defense Authorization Act as passed by the Senate. It is currently awaiting consideration in conference. If accepted, the amendment would prohibit all United States government agencies from purchasing or leasing telecommunications equipment and/or services from Huawei, ZTE, or any subsidiaries or affiliates. The language would also ban the federal government from using grants and loans to subsidize Huawei, ZTE, or any subsidiaries or affiliates. Finally, it would restore penalties on ZTE for violating export controls.

VI. Conclusion

New technology and information technology systems are integral components for small business operations. However, with technological advancements have come greater risks posed by foreign backed actors to compromise valuable information belonging to small businesses, as well as exploit vulnerabilities in the global supply chain to engage in criminal activities. Small businesses do not have the capacity to mitigate the threats posed by corporations like ZTE. Further, as Chinese backed firms flood American markets with cheap products, some small businesses could to become completely reliant on a bad actors' technology without knowing it. Protecting America's small businesses from illicit state-backed corporations should be a top priority.

---

[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*