Prepared Statement of Matthew G. Olsen

Hearing on "ZTE: A Threat to America's Small Businesses"

House Committee on Small Business

June 27, 2018

Chairman Chabot, Ranking Member Velázquez, and Members of the Committee, thank you for inviting me to this important hearing to discuss the risks that ZTE poses to the United States and our small businesses. I commend the Committee for addressing this issue, particularly in light of the broader cybersecurity and intelligence threats facing the United States.

At the outset, I want to recognize the important work of this Committee in promoting cyber security for our nation's small business community. As the Committee has recognized, advances in technology have offered small firms the opportunity to increase their productivity, and efficiency. But at the same time, these advances have opened the door for our adversaries to steal and destroy sensitive and valuable information that is critical to the continued success of small businesses. The Committee has worked to promote better coordination, education, and innovation with key stakeholders to address the evolving threat of cyberattacks. In particular, the Committee deserves praise for its work this year to promote information sharing on cyber threats and the training of cyber professionals in our workforce.

In my statement, I will first describe the overall cyber threat landscape, focusing on the nature and scope of the threat from China, and then discuss the risks posed by ZTE, as a Chinese-backed enterprise, to our national security interests.

I. Cyber Threat Landscape

As the Committee is aware, information networks are among our most valuable resources, critical both to our national security and our economic success. In this context, it is important to emphasize that the technology that supports these information networks is changing rapidly. For example, according to estimates, by 2021 the amount of information circulating the globe via IP networks will reach 3.3 zettabytes, and there will be 27.1 billion wireless and mobile devices, up from 17.1 billion in 2016.

We continue to witness an astounding rate of growth in the amount of unique, new information available worldwide, included significant increases in the velocity of data being transmitted and types of devices communicating information. With the advent of the Internet of Things (IoT) and the continued development and rapid iteration of technology, these trends are likely to continue to accelerate.

Small businesses will be at the forefront of this ongoing digital revolution. This is because small businesses have the agility and flexibility to create new products and to take advantage of advances in technology through rapid innovation and by bring products to market quickly. It is this very feature of technology startups—which nearly always begin as small businesses—that has turned the Silicon Valley and other technology centers from California to Maryland into major hubs of productivity and technological innovation.

With these advances in technology, there is a related and alarming trend in the scope and impact of cyberattacks. Such attacks now encompass both major disruptive attacks, as well as the use of actual destructive attacks on both public and private sector entities in the United States and abroad. For example, in 2012, we saw the advent of destructive attacks against Saudi Aramco, with over 20,000 computers affected, and a follow-on attack against Qatari RasGas. Similar attacks have recently been reported against the Saudi government.

In the United States, destructive attacks conducted by nation-states have hit private institutions, including the Las Vegas Sands Corporation and Sony Corporation. We have likewise seen significant disruptive attacks targeting U.S. financial institutions, including major attacks taking place multiple times in the last five years. Most recently, of course, Russian cyber-enabled efforts targeted our elections, including the 2016 presidential election.

In addition, to these destructive cyberattacks, the threat landscape is marked by massive data breaches affecting nearly every major economic sector, perhaps most prominently in the customer-facing sides of key retailers and health insurers. Most concerning is the increasing use of ransomware by organized criminal groups and small actors alike, seeking to hold data or systems hostage at a range of organizations across our nation, from hospitals to educational institutions. According to one report, the key sectors affected by ransomware include the services and manufacturing sectors, making up a combined 55% of ransomware infections.

Beyond these attacks, the threat landscape includes the ongoing theft of intellectual property from U.S. companies. In this regard, it is worth noting that the same network penetrations that permit threat actors to steal data can potentially be used to disrupt networks or destroy data.

The convergence of our systems and networks—whether we are talking about the increased links between industrial control systems and corporate networks or the proliferation of devices that are connected to the global network as part of the expansion of the IoT—only increases this vulnerability. An example of the practical implications of broad connectivity and convergence was the Mirai botnet turned household devices into a virtual IoT army and used them to execute a distributed denial of service attack on Dyn, a managed DNS and traffic optimization company that serves more than 3,500 enterprise customers.

From a broader perspective, it is important to understand that as a free society, we are relatively vulnerable to certain asymmetric threats, most notably from terrorist attacks and cyber-enabled attacks. While these two types of attacks are different in important ways, they bear certain basic similarities: Terrorist and cyber-enable attacks both are capable of having an outsized impact, where a single individual (or small group of individuals) can have a devastating effect on large numbers of people. These types of threats also are similar in the limited means available to prevent attacks in every instance. The government simply cannot be successful in stopping every small-scale terrorist attack, often carried out with little or no warning. Similarly, the government has limited capacity and authority to prevent the vast array of cyberattacks targeting our nation's private sector.

Indeed, our adversaries today do not have to attack our government to have a substantive strategic effect on our nation. Attacking civilian or economic infrastructure may be a more effective approach in the modern era, particularly for asymmetric actors like sophisticate hackers and terrorist groups. Our increasing reliance on digital, connected devices means that there are ways of having similar effects without the need for the large investment needed for conventional arms. Nation-states have long sought access to the critical systems of other nations for espionage, and we now see an expansion from these traditional activities to more aggressive actions by nation-states. The number of nations that possess the capability to exploit and attack continues to grow, with little incentive to act in accordance with appropriate state-to-state behavior.

Turning to the cyber threat from China, intelligence officials have repeatedly singled out China as among a small number of countries that pose the greatest cyber threats to the United States. In his Worldwide Threat Assessment this year, the Director of National Intelligence stated that, "China will continue to use cyber espionage and bolster cyber-attack capabilities to support national security priorities."

While the volume of attacks from Chinese government actors diminished after a bilateral agreement reached in 2015, intelligence officials and private sector experts continue to identify ongoing cyber activity from China. Indeed, in recent weeks, Chinese hackers have reportedly breached a U.S. Navy contractor that works for the Naval Undersea Warfare Center, stealing troves of data about submarine and undersea weapons technology. In addition, attacks in the last few months reportedly originating from China have also targeted US satellite and geospatial imaging firms, and an array of telecommunication companies. Thus, while Chinese hacking decreased after the 2015 agreement, cyber security analysts report, according to observers, that China's nation state hackers have retooled to be more stealthy and effective in their digital espionage operations, and recent attacks indicate that China is optimizing their plans to obtain valuable information.

Importantly, the intelligence community has found that most of the "detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide." This finding, of course, is directly relevant to the Committee's assessment of the risk posed by ZTE and other Chinese-backed firms.

China has focused its cyber espionage activities in a concerted effort to acquire U.S. intellectual property in order advance its economic and national security objectives. In this regard, the DNI stated this year that China "has acquired proprietary technology and early-stage ideas through cyber-enabled means." Similarly, in 2016, then-DNI James Clapper highlighted "the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas" and called this effort—again principally driven by China—a "persistent threat to

US interests." Former NSA Director Adm. Mike Rogers indicated that by the sheer "volume" of data taken, China is the largest cyber actor targeting the United States. Similarly, former Deputy Secretary of Defense Robert Work has testified that "we believe that Chinese actions in the cyber sphere are totally unacceptable as a nation-state," noting "we know that they have stolen information from our defense contractors."

II. The Risk from ZTE

Zhongxing Telecommunications Equipment, known as ZTE, is one of two Chinese companies, along with Huawei, that sells equipment for cellular networks. ZTE also makes smartphones sold in developing countries, as well as in the United States. ZTE reportedly has about 75,000 employees and operates in more than 160 countries.

The national security risks associated with ZTE and other Chinese-backed technology companies are well-documented. In an authoritative 2012 report, the House Intelligence Committee concluded:

> Private-sector entities in the United States are strongly encouraged to consider the long term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

In its report, HPSCI further recommended that the United States should "view with suspicion" the continued penetration of the U.S. telecommunications by Chinese technology companies. The Committee urged: "U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment in their systems."

The concerns underlying the HPSCI caution regarding ZTE were multifold: First, the Committee observed that, given the reliance of the United States on interdependent critical infrastructure systems, a disruption in telecommunication networks could have a devastating impact, causing shortages and stoppages that ripple throughout society. Second, the Committee cited the vulnerabilities—ranging from insider threats to cyber espionage—associated with foreign-sourced telecommunications supply chains used for U.S. national security applications. Finally, as the Committee found, "the U.S. government must pay particular attention to products produced by companies with ties to regimes that present the highest and most advanced espionage threats to the U.S., such as China."

More recently, intelligence leaders reaffirmed the risks that ZTE poses to U.S. national security. In February, the intelligence community heads all recommended avoiding technology products from Chinese companies, like ZTE and Huawei. As FBI Director Chris Wray testified, "We're 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." Such access "provides the capacity to exert pressure or control over our telecommunications infrastructure," Wray said. "It provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage." Former NSA Director Michael Rogers observed, "This is a challenge I think that is only going to increase, not lessen over time for us. You need to look long and hard at companies like this."

Similarly, in April the Defense Department determined that ZTE posed an "unacceptable risk" and banned sales of ZTE cellphones on military bases. The same month, officials in the United Kingdom cautioned that using ZTE equipment was so problematic that national security concerns "cannot be mitigated."

For its part, ZTE has proven to be a particularly bad actor, flouting U.S. export control laws and deceiving regulators. In 2016, the U.S. government found that ZTE violated U.S. sanctions against Iran and North Korea, by using various U.S. components in systems it sold to those two countries. When the Commerce Department released its findings against ZTE in 2016, it disclosed evidence of the company's guilt. One document, signed by several senior ZTE executives, reportedly cautioned that American export laws were a risk because the company was selling to "all five major embargoed countries — Iran, Sudan, North Korea, Syria and Cuba." A second company document featured details on best practices to circumvent American sanctions.

In the settlement agreement with the government, ZTE admitted that the company's "senior leadership had been developing, and in fact did develop and adopt in whole or in part, a company-wide scheme to evade U.S. economic sanctions and export control laws. [ZTE's] actions were developed and approved by the highest levels of its management, and entailed the use of third-party companies to both conceal and facilitate its business with sanctioned jurisdictions, including Iran." Last year, ZTE acknowledged its guilt and paid a $1.19 billion fine.

Then, in April, the Commerce Department further penalized ZTE for violating its agreement with the United States by lying to government officials both during negotiations and after the settlement. Commerce found that ZTE "engaged in an elaborate scheme to prevent disclosure to the U.S. Government, and, in fact, to affirmatively mislead the Government." The Commerce Department concluded that, "The provision of false statements to the U.S. Government, despite repeated protestations from the company that it has engaged in a sustained effort to turn the page on past misdeeds, is indicative of a company incapable of being, or unwilling to be, a reliable and trustworthy recipient of U.S.-origin goods, software, and technology." As punishment, the government prohibited U.S. technology companies from selling their products to ZTE for seven years.

Finally, earlier this month, the Commerce Secretary intervened and announced a deal to lift the sanctions against ZTE. The company agreed to pay a $1 billion fine and fund a new in-house compliance team staffed by U.S. experts. This latest agreement, however, has drawn bipartisan criticism in Congress. Last week, the Senate voted to reinstate the penalties on ZTE. And a bipartisan group of Senators released the following statement: "We're heartened that both parties made it clear that protecting American jobs and national security must come first when making deals with countries like China, which has a history of having little regard for either. It is vital that our colleagues in the House keep this bipartisan provision in the bill as it heads towards a conference."

* * *

The controversy over ZTE is dynamic and complex. From my perspective, the critical national security concern going forward is the risk that ZTE and other Chinese-backed technology firms may pose to U.S. telecommunications and other critical infrastructure—risks that Congress and the intelligence community have amply documented. Moreover, ZTE has proven to be particularly untrustworthy, as it seeks to do business in the United States and with U.S. technology companies.

Thank you for the opportunity to participate in this important hearing. I look forward to your questions.