ZTE: A THREAT TO AMERICA'S SMALL BUSINESSES

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

HEARING HELD
JUNE 27, 2018

Small Business Committee Document Number 115–082
Available via the GPO Website: www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–507 WASHINGTON : 2019

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
TRENT KELLY, Mississippi
ROD BLUM, Iowa
JAMES COMER, Kentucky
JENNIFFER GONZALEZ-COLON, Puerto Rico
BRIAN FITZPATRICK, Pennsylvania
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
JOHN CURTIS, Utah
NYDIA VELÁZQUEZ, New York, *Ranking Member*
DWIGHT EVANS, Pennsylvania
STEPHANIE MURPHY, Florida
AL LAWSON, JR., Florida
YVETTE CLARKE, New York
JUDY CHU, California
ALMA ADAMS, North Carolina
ADRIANO ESPAILLAT, New York
BRAD SCHNEIDER, Illinois
VACANT

KEVIN FITZPATRICK, *Majority Staff Director*
JAN OLIVER, *Majority Deputy Staff Director and Chief Counsel*
ADAM MINEHARDT, *Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

ZTE: A THREAT TO AMERICA'S SMALL BUSINESSES

WEDNESDAY, JUNE 27, 2018

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 11:02 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Brat, Radewagen, Kelly, Bloom, Curtis, Velázquez, Evans, Lawson, Adams, and Schneider.

Chairman CHABOT. The Committee will come to order.

We want to thank everyone for being here this morning.

Today we are here to discuss a topic that has garnered quite a bit of attention in recent months. However, it is an issue that this Committee has paid very close attention to for a number of years now. That is the looming threat of Chinese telecommunications giant, ZTE.

As this Committee has learned through past hearings, foreign-backed entities from countries like China and Russia regularly target small businesses to steal intellectual property and undermine America's critical infrastructure. The FBI has already determined that foreign state actors pose a serious cyber threat to the telecommunications supply chain. It is also clear that many foreign nations are responsible for direct cyberattacks on the United States in an effort to steal intellectual property and sensitive personal information.

In a report by our colleagues on the Intelligence Committee, U.S. businesses and cybersecurity experts have reported persistent attacks that could be traced back to China and were thought to be supported by the Chinese government. And studies from the Department of Defense have warned of the difficulties associated with defending against threats posed by foreign nations, stating that, "[the] means and opportunity [for nation-state adversaries] are present throughout the supply chain and lifecycle of software development." This is particularly troublesome for small businesses that not only rely on products from, but also engage in commerce with, globalized telecommunications firms in countries like China. Hearings by this Committee have shown that small businesses have become top targets for nefarious state-backed actors because they tend to be the softest targets. They have fewer resources to manage their information technology systems and respond to cybersecurity incidents, and they often lack the technical knowledge needed to assess the ever-evolving threats. Additionally, most small busi-

nesses do not have a lot of money to throw around and thus, may often purchase less expensive tech products often produced by large Chinese firms. This is a recipe for disaster.

Now, let me be clear. I do not believe for a minute that an American small business owner would purposely buy a product that puts their own operations at risk, let alone jeopardize our national security. However, the problem is that most small businesses will not even know that they are using a product or service that has been provided by a nefarious actor. Nor should they. Their job is to run their business, employ hardworking Americans, and keep their customers happy.

When we talk about existential threats to national security—and that is what ZTE is—it is the Federal government's job to protect Americans and American small businesses.

That is exactly what happened in April of this year when ZTE was effectively banned from doing business in the U.S. After years of investigations and deliberations into the ZTE case, after ZTE was afforded its due process in this country (a favor I might add that usually goes unreturned to American companies in China), and after numerous second chances, the Trump administration rightfully made the decision to finally hold ZTE accountable, a move that many of our colleagues on both sides of the aisle applauded.

Now, we face the very real possibility that ZTE may be given yet another chance. Commerce Secretary Wilbur Ross announced earlier this month that a new agreement had been reached with ZTE, and after paying over a billion dollars in penalties and forfeitures, the Bureau of Industry and Security will remove ZTE from the Denied Persons List and they can return to business as usual.

I am very concerned that this decision could ultimately put Americans at risk. ZTE has consistently lied to this administration, and it is reasonable to assume that it will do so again.

Today's hearing will examine the threat posed by ZTE to American small businesses, if ZTE is allowed to re-engage in the American economy. This is an important decision that impacts both our national security and our economic security, and I believe it demands much more attention than it has received so far.

I think we all look forward to hearing from our witness about this threat this morning and how we can better guard against any of those issues.

And I would now like to yield to the Ranking Member for her opening statement.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. And thank you really for holding this critical hearing.

As we have seen time and again, in this committee and in national headlines, cybersecurity affects every facet of our lives. To this day, many of us remain deeply troubled about how an adversarial foreign power influenced our nation's 2016 election results and whether we will be prepared to prevent similar actions in the future.

We have also heard in this committee, that small businesses are uniquely vulnerable to cyberattacks, whether it be from small-time cyber criminals or foreign powers intent on industrial sabotage, such as China and Russia.

As one of the world's largest telecommunications equipment manufacturers, ZTE occupies a unique and dangerous space when it comes to many of these issues. An increasing number of consumer and business devices, like cars, appliances, communication networks, utilities, and phones, rely on smaller components manufactured by ZTE and other similar Chinese companies. The prevalence of ZTE's products is disturbing when we realize that the company has a history of being a national security threat to American interests. Concerns about ZTE date back to 2012 and those issues continue today.

That is why this administration must take that threat posed by ZTE and other Chinese companies seriously. Unfortunately, it appears that the president seems intent on weakening our security posture when it comes to responding to this threat.

The government has previously taken some steps to protect itself in this area. In April, the Commerce Department banned U.S. companies from selling parts or providing services to ZTE, virtually shutting down the company. In May, the Pentagon pulled ZTE phones from stores on U.S. military bases because they consider them a security threat.

However, on June 7th, the president largely reversed these moves, agreeing to lift sanctions reportedly ignoring the advice of the U.S. intelligence community and many American economy advisors.

Our national security cannot be imperiled by lax policy toward these hostile actors. Where the administration is taking unacceptable risks, Congress must step forward to contend with these illicit Chinese government-backed enterprises.

Fortunately, the first legislative steps have been taken to correct the administration's careless approach. The Senate recently approved an amendment to the National Defense Authorization Act, that if enacted will reinstate sanctions, eliminating ZTE and Huawei access to U.S. suppliers.

Sadly, President Trump is working with Senate republicans to undermine this effort. Without such restrictions, these Chinese companies can have major and costly implications for small businesses and their ability to operate, and it is irresponsible to ignore the threat and undermine the very interests Congress is here to protect. Clearly, cybersecurity is central to protecting both our national and economic security.

During today's hearing, we will explore the critical issues facing small businesses in cyberspace and the dangers they face when actors with ill intent are afforded unfettered access to U.S. markets. It is my hope that today's discussion helps shed light on how Congress can work to protect our small businesses and our country from bad actors operating in cyberspace.

I would like to thank the witnesses again for being here, and I yield back. Thank you.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

And if Committee members have opening statements prepared we would ask that they be submitted for the record.

And I will take just a moment to explain our rules and lighting system here. We operate under the 5-minute rule. Each of you gets

5 minutes to testify. The lights are there to kind of assist you. The green light will be on for 4 minutes. The yellow light will be on for a minute to let you know that it is about time to wrap up. And then the red light will come on saying that your time is up. So if you could stay within those parameters we would greatly appreciate it. We also apply those rules to ourselves, so we all get 5 minutes to ask questions as well.

I would now like to introduce our distinguished panel here this morning. We will begin with Mr. David Linger, who has over 25 years of learning and success in bringing new technologies and innovations to market through roles in engineering, product development, product management, and business development. Mr. Linger currently serves as the President and CEO of TechSolve, Inc., which happens to be in my home district in Cincinnati, Ohio. His team of experts has leveraged its deep rooted knowledge in machining, data extraction, and the manufacturing process to translate emerging technologies into every day manufacturing and business solutions for small businesses. And we welcome you here today, Mr. Linger.

Our next witness will be Andy Keiser, who comes to us as a Visiting Fellow from the National Security Institute. Previously, Mr. Keiser served 14 years on Capitol Hill for former House Intelligence Committee Chairman Mike Rogers, as Chief of Staff, Legislative Director handling Cybersecurity and Energy and Commerce Committee issues, and as senior advisor to the Intelligence Committee. And we welcome you here, Mr. Keiser.

I would now like to yield to the Ranking Member for the purpose of introducing our third and final witness.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

It is my pleasure to introduce Mr. Matthew Olsen, Cofounder and President of IronNet Cybersecurity, a network security company in Maryland. Mr. Olsen is a graduate of the University of Virginia and Harvard Law. He began his distinguished career as a trial attorney for DOJ's Civil Rights division, and then as a federal prosecutor for the U.S. Attorney's Office for D.C., where he served as the first Director of the Office of National Security Division. Mr. Olsen has worked in the DOJ's National Security Division, and went on to serve as the Associate Deputy Attorney General and as the General Counsel of the National Security Agency. In the Obama administration he served as the Director of the National Counterterrorism Center, and is currently a member of the Homeland Security Advisory Council. Thank you for being here.

Chairman CHABOT. Thank you very much.

Mr. Linger, you are recognized for 5 minutes.

STATEMENTS OF DAVID LINGER, PRESIDENT & CEO TECHSOLVE, INC.; ANDY KEISER, VISITING FELLOW, NATIONAL SECURITY INSTITUTE, ANTONIN SCALIA LAW SCHOOL, GEORGE MASON UNIVERSITY; MATTHEW G. OLSEN, PRESIDENT, IRONNET CYBERSECURITY

STATEMENT OF DAVID LINGER

Mr. LINGER. Thank you very much.

Chairman Chabot, Ranking Member——

Chairman CHABOT. If you could turn the mic on that would be great. Thanks.

Mr. LINGER. Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for inviting me to testify this morning on behalf of the U.S. small manufacturers regarding the impact that cyberattacks on this critical national asset.

Only the government tops the manufacturing sector (followed by finance and healthcare) as the most targeted sector by cyber espionage. These aggressors are seeking to disrupt manufacturing not only through the ceiling of intellectual property, but also the destruction of the U.S. supply chain by crippling them both financially and through attacks on their intelligent machines.

Rebecca Taylor, Senior Vice President for the National Center for Manufacturing Sciences (NCMS) stated, "Every manufacturer is at risk. It is not a matter of if they will be targeted; it is a matter of when."

A 2017 Ohio Manufacturing Extension Partnership (OH MEP) survey of Ohio manufacturers revealed that only 12.5 percent of manufacturers responded that they understand what cybersecurity is and have worked to protect their machines, intellectual property, and IT systems and only 4.5 percent have undergone a cybersecurity assessment.

According to 2015 Census data, the vast majority of manufacturers are very small. Of the 250,000 firms in the U.S. manufacturing sector, only 1.5 percent of those manufacturers have greater than 500 employees, 188,000 have less than 25 employees.

As President of TechSolve, I have a very unique perspective of the devastation these cyberattacks have caused our customers. I am here today to share the story of one such manufacturing company that has experienced these attacks and exemplifies the risks a majority of these manufacturers face on a 24/7 basis. To Tony Strobl, President of Cincinnati Crane & Hoist, these cyberattacks are a war on his company and his employees. Cincinnati Crane is a very small, 20-person company, based in Southwest Ohio, that supplies turn-key crane systems, parts, and services. Cincinnati Crane is a veteran-owned business that has seen growth of more than

400 percent in the last three years and was awarded the U.S. Department of Commerce Export Achievement Award in 2017.

Earlier this year, Tony's company was the victim of social engineering, or more specifically a spear phishing campaign that contained malicious macros that breached their email system; went undetected for an uncertain amount of time; embedded hidden folders within Office365; "spoofed" legitimate invoices that were being emailed to Cincinnati Crane's customers; replaced those invoices with bogus invoices providing false banking information that ultimately syphoned over $200,000 from his customers.

When the Cincinnati Crane invoices had aged 30 days and collection calls were made, customer after customer told Cincinnati Crane that they had already paid their invoices. The $200,000 that was stolen from Cincinnati Crane is now unrecoverable according to the FBI. Due to Cincinnati Crane's current financial standing, Tony had to make the devastating decision to lay off four of his employees, 20 percent of the company.

Not only has this cyberwar affected those families, but it has severely hampered Tony's ability to complete customer orders, grow, and innovate.

Cincinnati Crane's customers are afraid to conduct business with Tony. Not only are they concerned about sensitive drawings and corporate data that they have shared with Tony's project managers, but they are also afraid to open email correspondence, even making payments electronically with Cincinnati Crane. Even though TechSolve and its IT sub-contractors have scrubbed their systems and are working on long-term cybersecurity policies and procedures through remediation and adaptation of the NIST SP 800-171 cybersecurity controls, the effects of these cyberattacks continue to threaten its long-term viability.

The Cisco 2018 Security Capabilities Benchmark Study further corroborates data that TechSolve has observed when it comes to manufacturers in general, but especially small manufacturers. There will be more operational technology (OT) or internet of thing (IOT) attacks in the future.

Cyberattackers can hack into machine tool accessories or machine tools and alter the program. Therefore, either stopping the manufacturer from providing the right parts to their suppliers, or even worse, altering the quality of the part that is a portion of a larger assembly, thus compromising the entire system.

For large defense primes and original equipment manufacturers (OEMs), it is critical for their supply chains to protect the integrity of that digital thread.

There are a number of ways to entice companies to begin implementing cybersecurity best practices and the DOD has done a great job by leading the way and establishing one method, regulation through the current DFARS and NIST SP 800-171 controls. The current shortcoming is a lack of validating testing.

TechSolve is working with several manufacturing companies that are conducting business with the DOD. They are technically "in compliance" with the DFARS; however, this does not make them cyber secure.

Another approach is being discussed in the State of Ohio. The Attorney General is working with the Senate and House on former Senate Bill 220. This "safe harbor" bill, if passed, will create a law that will protect companies that can prove that they have proactively implemented and are maintaining cybersecurity measures within their systems.

Research conducted by the National Cyber Security Alliance states that there was a 600 percent increase in IOT attacks from 2016 to 2017 and that the number one country of origin is China at 21 percent. Given these statistics, and the fact that 60 percent of small and mid-sized businesses that have been hacked shut down within 6 months of the attack, it is imperative for all of us that we safeguard this incredible important industry sector. Thank you.

Chairman CHABOT. Mr. Keiser, you are recognized for 5 minutes.

STATEMENT OF ANDY KEISER

Mr. KEISER. Thank you, Mr. Chairman, Ranking Member Velázquez, distinguished members of the Committee. If you will forgive me, I am used to sitting in the back along with these guys as a staffer not in direct line of fire to you guys, so go easy on me. But pleasure to be here.

I will start with a story that I think you all will immediately relate to. My former boss, as you mentioned, Chairman, Mike Rogers, first became interested in the activities of ZTE and Huawei not because he was a former U.S. Army officer or because he was a former FBI agent, or even because he was on the Intelligence Committee. He actually got interested in those companies because a Michigan company, similar to Mr. Linger here from Ohio, came to him with a problem.

So as all of you would do, he listened to that small business owner very carefully. What he was doing was building cell towers in sort of the hinterlands of Michigan, out in the thumb as we would call it. And he found companies, Chinese companies were coming in at a price that was astonishing to him. So he would offer a bid and these companies, Huawei and ZTE would come in not just blew his bid, but below the cost of what the materials were to build the towers.

So that got a former FBI agent thinking, why on earth would these companies be doing that? More on that later.

As I do not need to remind this room, small business is the lifeblood of the economy. Two out of every three new private sectors jobs are created by small business. It is inherently creative, resilient, and able to adapt quickly to market conditions, but one thing it is not able to do is respond to Nation state attacks, aggressive, unrelenting espionage with theft of trade secrets. Those are exactly the challenges presented by ZTE and Huawei.

A little history on China I think is important for the Committee. For thousands of years, China, of course, viewed itself as superior to all other world powers. Following an self-described century of humiliation resulting from imperialist incursions from the West and Japan, it now seeks a return to that perch under the consolidated leadership of President Xi Jinping, newly pronounced President for Life, China intends to become a global economic, military, and technological leader rivaling or surpassing the United States really in the next 10 to 15 years.

There are some troubling indicators to this. The Chinese GDP is scheduled to surpass that of the United States by 2029. The Chinese military is rapidly modernizing and they are directly aiming their capabilities at U.S. strengths. That includes cyber, sea power, and space.

Part of their grand vision, of course, includes the Made in China 2025 strategic plan where they will become the world's leader in high-tech fields squarely within the expertise of ZTE and Huawei.

Those two companies that we are discussing today are working fast to put western vendors out of business to secure market dominance. In just 7 years, Huawei has actually gone from an afterthought with poorly functioning equipment and only 10 percent market share, to the top position in lucrative business like LTE radio.

Excluding the United States, Huawei actually has a 38 percent total market share globally. By investing heavily in R&D, which they are doing but perhaps more concerning by stealing their way to some innovation, they have achieved this market position. Actually, Huawei has admitted to stealing router products, secrets from Cisco, all the way down to the typos in the manual. Huawei apparently has stolen the design for the iPhone right down to the last screw.

As mentioned earlier, I worked on the House Intelligence Committee, and we issued a report back in 2012. Many of those findings still hold true to this day. In 2012, the report stated the risks associated with Huawei and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national security interests.

Perhaps more relevant to this Committee, the report suggested the risks associated with doing business with either ZTE or Huawei for equipment or services were certainly not recommended.

We can discuss the denial order by the Commerce Department in some detail, but it was pretty hard hitting. Among other things, specifically to ZTE, the Commerce Department stated that ZTE demonstrated a pattern of deception, false statements, and repeated violations. In fact, they admitted to committing 380 violations and engaged in an elaborate scheme to prevent disclosure to the U.S. government.

Look forward to getting into some more details in Q&A but Chairman Rogers and Ranking Member Ruppersberger at the time teamed up again to write an op ed in the Wall Street Journal earlier this year which called the threat from ZTE a clear and present danger to U.S. national security. I agree completely with this and encourage this body and the rest of the Hill to respond accordingly. Thank you very much for the time.

Chairman CHABOT. Thank you very much, Mr. Keiser.

Mr. Olsen, you are recognized for 5 minutes.

STATEMENT OF MATTHEW G. OLSEN

Mr. OLSEN. Thank you, Mr. Chairman, and Ranking Member Velázquez, and members of the Committee. I really appreciate the opportunity to be here for this important hearing. And I would like to commend the Committee for addressing this issue, particularly in light of the cybersecurity and intelligence challenges facing the country. And at the outset, I would also like to recognize the important work of this Committee in promoting cybersecurity more broadly for our nation's small business community. You have done some really important work.

In my brief statement I will first just describe the overall cybersecurity threat landscape, focusing in particular on the threat from China, and then I will discuss in particular the risks posed by ZTE as a Chinese-backed enterprise to our national security.

First, as the Committee is well aware, small businesses are at the forefront of our ongoing digital revolution, and this is because small businesses have the agility and flexibility to create new products and to capitalize on advances in technology. But with these advances in technology, there has been a related and really alarming trend in the scope and impact of cyberattacks. Such attacks

now encompass both disruptive and destructive type of attacks on both our public and private sector networks as Mr. Linger and Mr. Keiser have both addressed.

In addition to these types of attacks, disruptive and destructive, the threat landscape is also marked by massive data breaches. Most concerning is the use of ransomware. We have seen an increase in ransomware, especially hitting small businesses over the past few years, and these have hit hospitals, educational institutions, and manufacturing companies.

Beyond these attacks, the threat landscape also includes the ongoing theft of intellectual property, and again, Mr. Keiser talked I think quite persuasively about that.

You know, from a broader perspective, it is important to recognize that as a free society, we remain just vulnerable to asymmetric attacks, whether that is from terrorist organizations in the United States or from cyber-enabled attacks from a range of actors online. Nation-states have long sought access to the critical systems of other nations for espionage and we are seeing an expansion from these traditional activities to a more aggressive, as I said, destructive attacks from Nation states.

Now, just looking at China in particular, our intelligence officials have repeatedly singled out China as one of the small number of nations around the world that pose the greatest threat to us in cyber. In the worldwide assessment, the director of National Intelligence said that China will continue to use cyber espionage and bolster cyberattack capabilities to support national security priorities. That was just in February of this year.

And while the overall volume of attacks from Chinese government actors diminished right after 2015, there was a bilateral agreement between the United States and China, recently, nation-state hackers from China appear to have reorganized and retooled in a way that makes them more stealthy and actually more effective in their espionage operations, and recent attacks indicate that China is really optimizing their plans to continue to obtain very valuable information from both the government and our private sector.

All right. So turning from China and the cyber threat landscape to ZTE in particular, in the authoritative report from 2012 that Mr. Keiser referenced from the House Intelligence Committee there I think, again, that remains the touchstone for any review of Huawei and ZTE. The Committee concluded that based on both classified and unclassified information, Huawei and ZTE, I quote, "cannot be trusted to be free of foreign state influence, and thus pose a security threat to the United States and to our systems."

And now more recently, just this past year, intelligence leaders reaffirmed in testimony to Congress that ZTE poses a threat to our national security. In February, all of the intelligence community heads unanimously found or recommended that we avoid technology products from both ZTE and Huawei. The FBI director testified that ZTE's access to our networks pose a challenge because of their capacity, one, to exercise control over our networks, to steal information, and to conduct undetected espionage. So all three of those are risks.

And we are not alone. The United Kingdom recently cautioned against the use of ZTE equipment.

Now, for its part, as we have heard ZTE has proven to be a particularly bad actor, flouting U.S. export laws and deceiving regulators, and for that they have been fined and sanctioned. So I look forward to talking more about that.

I would say in sum that from my perspective the critical security concerns for us is the risk that ZTE and other Chinese-backed organizations pose to our critical infrastructure. Given that ZTE has proven to be particularly untrustworthy, I believe that it poses a clear and significant risk to our national security.

So I thank you for the opportunity to be here and look forward to your questions.

Chairman CHABOT. Thank you very much.

And I will recognize myself for 5 minutes to begin the questioning.

Mr. Keiser, I am going to go to you first. You had talked about in Michigan, the cell towers going up below the cost of materials. So where does that end up, that story?

Mr. KEISER. So I think where does it end up? He lost the bid, the small business owner. So Huawei and ZTE are out in some of our rural areas. Some of the providers use them. They are, as Matt knows extraordinarily well, they are thankfully nowhere near our Five Eyes network, the intelligence sharing agreement that we have with Australia, New Zealand, the UK. And so that is where that ended up. But I think the important fact there was it proved that Huawei and ZTE are not in this for profit. Unlike any other western company, they are not beholden to shareholders. This is a strategic plan by the communist Chinese government to at least have the capability to collect information around the world, and perhaps more concerning, to turn off a switch in the event of a potential conflict and create havoc that we do not even want to think about on this Committee.

Chairman CHABOT. So just to make one point, the motivation, the goal of companies like ZTE, Huawei, are different than those that are say on the New York Stock Exchange or publicly held who have a profit motive who are competing with each other; this is more of a national security or something that they are trying to accomplish that is a goal of the Chinese government. Is that right?

Mr. KEISER. That is right. I will give you an example. In the last two weeks, after the United States of America issued a denial order prohibiting them from purchasing any U.S. components, which essentially would have put them out of business, the two biggest Chinese state-owned banks infused $11 billion to keep them afloat. Name a western company that might have that option.

Chairman CHABOT. Mr. Olsen, let me ask you a question. Do you believe that ZTE is a threat to America's small businesses? Is it something that they should be concerned about as well? And if so, why?

Mr. OLSEN. I absolutely do. I believe that ZTE poses a threat, you know, more broadly, but also in particular to America's small businesses. The key I think, as we started to address is that as a Chinese-backed organization company, it essentially is in the position to advance the national interests of China. And we have seen

from the broader features of China and how it has acted in cybersecurity, in the cyber landscape stealing information from the United States. Because ZTE is in a communications infrastructure company, it would put ZTE in a position to carry out those interests for China, whether it is to disrupt our infrastructure or to potentially steal information. So from that perspective I do think it is a threat.

Chairman CHABOT. Mr. Linger, you had mentioned a couple of statistics in your testimony. I think one that you mentioned that the number of attacks had gone up in recent years pretty substantially and then the principal bad actor in this was a Chinese entity of one form or another. And I think third, that 60 percent of small businesses that undergo one of these cyberattacks are out of business within 6 months according to your testimony. Could you touch on those, if you want to expand up on those a little?

Mr. LINGER. I think a bit of a perfect storm is you have the sophistication of the attacks and the hackers, combined with this move to digital manufacturing, this move to an internet of things where now more and more information is on the systems in the shop. And now those are not protected. That is now vulnerable. And that is where we are seeing an increase, even if a company is protecting their front office, if you will, they may not be protecting all the designs and the models and the data that is on their machines, and that is what is happening.

Chairman CHABOT. Thank you.

In the little time I have got left, let me go back to you, Mr. Olsen. I think, and you referred to this, in April of this year, the United Kingdom considered products manufactured by ZTE to be a significant national security risk. In that same month, the Department of Defense banned sales of ZTE wireless products on military bases. And I think the Ranking Member mentioned that.

Considering our own military and the militaries of our allies that they have determined these products to be at risk, again, is that of particular concern to somebody, say to small businesses of this country who do not have the same sophisticated technology protecting them?

Mr. OLSEN. Yes. Absolutely. I mean, again, the core national security concern does involve our national security systems, our military systems, intelligence systems, classified systems, and those of other allied countries, like the United Kingdom. But that concern certain emanates out from those core intelligent systems to encompass small businesses. Because of the nature of our networks and how closely they are linked, a threat even at a small business can pose a national security threat to the country.

Chairman CHABOT. Thank you very much.

And the Ranking Member is recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you.

Mr. Olsen, we know that companies like ZTE and Huawei, which have the capacity to maliciously modify or steal information and conduct undetected espionage, have a large global presence. How can we protect ourselves from these companies acting here in the U.S.?

Mr. OLSEN. So I think in the instance of Huawei and ZTE, what we have seen is we have actually seen government action to help

protect the country. The sanctions regime that is in existence for protecting our interests in terms of how our technology is shared around the world, that is part of the regime that ZTE violated in selling products that contain U.S. protects to Iran and North Korea. Admittedly, it violated those.

So the enforcement of those sanctions regimes is one way that we can protect ourselves. We certainly can protect ourselves by imposing limitations at a government level, government agencies, military, our U.S. military as we have seen purchasing those products because of the risk that they pose. But I think, you know, I would say two more things. One, better, and again, Mr. Linger discussed this, the hardening of our cybersecurity because the threat comes from these companies but it comes much more broadly than that so that small businesses need to up their game when it comes to cybersecurity. And then fourth, again, just the work of this Committee and Congress in bringing attention to this issue.

Ms. VELÁZQUEZ. But is it not a really bad proposition when we are taking all these steps but at the same time the administration is sending a different message? So we are warning them that we are watching, but on the other hand, we are saying we are going to do everything we can to help them?

Mr. OLSEN. Yes. I would tend to align my views with those recently expressed by Senator Warner and Senator Rubio in a bipartisan expression of their view about where we should be with respect to ZTE and the imposition of sanctions. And I do think that ZTE in particular has proven itself to be not trustworthy both in the sanctions violations, but also directly in their statements which turned out to be false to the U.S. government during those negotiations in the settlement.

Ms. VELÁZQUEZ. Thank you.

Mr. Linger, as you discussed in your testimony, small business manufacturers have made the shift to utilizing smart machines that store data. Yet, this adds another layer of risk for businesses, especially when the machines use components made by companies like ZTE. Can you describe how this backdoor access can be used nefariously and what steps small manufacturers can take to protect themselves?

Mr. LINGER. That is a great question. I think certainly, as companies, manufacturers and small manufacturers, for them to compete nationally and internationally, they have got to up their game in terms of the digital manufacturing. They have got to be connected. They have to gain all the efficiencies that are available when all the machines are connected and talking to one another and real time data is being used to drive that production site. That is what is driving this use of information real time on the plant floor. That is your point and now you are exposed. Right?

Ms. VELÁZQUEZ. Right.

Mr. LINGER. So you have to connect all the data, and protect at the same time. And so, so much of it is awareness and understanding that that data is there and it is vulnerable. And to put technology and action in place to protect it.

Ms. VELÁZQUEZ. Thank you.

Mr. Keiser, in your testimony you brought up the concern that Chinese-backed companies can undercut independent American-

owned small companies. What is at risk when small businesses are competing with government-based competition?

Mr. KEISER. Right. Good question. I think it is impossible for them to do. Right? You have this massive theft of intellectual property. You also have forced technology transfer that the Chinese participate in. All of this undermines U.S. companies' ability to innovate, create jobs, come up with the next fancy gizmo we might be carrying in our pockets, and that just makes it harder for them to pull that off.

Ms. VELÁZQUEZ. Thank you.

Mr. Olsen, you noted that ZTE reportedly has about 75,000 employees and operates in more than 160 countries. What does ZTE's operation look like in the U.S., and how many of those 7,000 employees are in the United States?

Mr. OLSEN. So I know from reports that ZTE has focused its cellphone sales in developing countries primarily, so outside the United States. But it does have a substantial presence here and that is partly the concern. I do not have a specific number on the employees.

Ms. VELÁZQUEZ. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentleman from Iowa, Mr. Blum, who is the Chairman of the Subcommittee on Agriculture, Energy and Trade is recognized for 5 minutes.

Mr. BLUM. Thank you, Chairman Chabot. Thank you for our witnesses for being here today.

And Mr. Chairman, I have noticed lately we have had a lot of witnesses from Cincinnati, Ohio. Is that a coincidence?

Chairman CHABOT. They are just the best witnesses, do you know what I mean? We love all our witnesses from all over the country.

Mr. BLUM. I would like to talk for a few minutes about the cloud. I know increasingly small businesses are moving to the cloud. The president of my small business just informed me a couple weeks ago that we are going to the cloud. And the Department of Defense, I believe, is going to the cloud. Is cloud-based computing more secure or less secure, particularly for small businesses? It is kind of a nebulous thing and I am really curious to what your answers are on this. So anyone, or all that want to take a shot at this, please go ahead.

Mr. KEISER. So good question. I worry a bit about the cloud. I worry about having a consolidation of information that the right set of keys can get into. I think OPM comes to mind, a massive breach. I worry about the Pentagon coming up with one giant cloud to house all of its unclassified information. I am actually skeptical they will be able to pull that off, actually. Most Fortune 500 companies have an average of eight clouds. So you might have a Microsoft cloud running your Outlook and your Office applications. You might have——

Mr. BLUM. Is that due to security concerns?

Mr. KEISER. It is due to functionality, typically, actually. So I worry a little bit about that but curious if Matt has a different view.

Mr. OLSEN. I share your concerns there. I work at a technology firm and one of the engineers in my company has a sign above his computer. It says, "There is no such thing as the cloud. It is just someone else's computer."

Mr. BLUM. That is great. That is great. Yeah.

Mr. OLSEN. To sort of make the point that it really depends. And this security in the cloud is only as safe as the cloud-based security. Now, there are some efficiencies that can be gained from a security perspective where the data is together, and if you are in a very secure cloud environment that can be more secure than having information spread out on a number of insecure nodes or laptops or computers; right? So there are some potential advantages. Certainly, there are other functionality advantages to having applications run in the cloud that companies are increasingly taking advantage of.

So the last thing I would just say is security in the cloud is a critical issue because, as you point out, sir, this is a trend that is going to continue, that we are going to continue to see migration to the cloud. The government is doing it. The private sector is doing it.

Mr. BLUM. How secure is the cloud? How secure is it?

Mr. OLSEN. Again, some companies are very secure. The major companies that——

Mr. BLUM. But some are not?

Mr. OLSEN.—yeah, that have moved directly into the cloud I think are secure. The government itself is working with Amazon, for example, in the intelligence community. So they have managed to, obviously, make that secure enough to work for the intelligence community.

Mr. BLUM. But a small company going to a cloud provider could be opening themselves up if that provider cuts corners, particularly on security; correct?

Mr. OLSEN. I think that is right. I think that is why it is just so important to be vigilant regardless of where you keep your data and your applications.

Mr. BLUM. Mr. Linger?

Mr. LINGER. I would say that in so many cases for a small manufacturer, they are better off in the cloud. The security measures there are immensely better than what they have on their one server in their back room of their shop. Now, obviously, if they are doing the things right, maybe you would not say that, but I would say 80 percent of the companies that I see are so insecure in how they handle their data on their plant floor that the cloud is safer. And that may change over time.

Mr. BLUM. Thank you for that.

This is a very simple question. Should ZTE be banned from doing business in the United States? Let's not worry about what the administration is doing. What is your opinion?

Mr. KEISER. So, I mean, I think clearly, from doing business in the United States? Unequivocally yes. Whether they should be completely put out of business around the world is another question. To be fair though, the steps taken in the last couple years are far more significant than we had seen in the previous three administrations I would say.

Mr. BLUM. Mr. Olsen?

Mr. OLSEN. Yes. I mean, I think I agree with the position that the government took when it prohibited U.S. technology companies from selling their companies to ZTE. That was part of the sanctions regime. And I think that there certain should be—I would take seriously the advice of the intelligence community saying that people should not use ZTE products.

Mr. BLUM. Mr. Linger?

Mr. LINGER. Yeah. It comes down to the actual devices themselves and where is the device, where is it placed, and what can it do? Understanding at that technical level.

Mr. BLUM. Thank you for your insights. I yield back, Mr. Chairman.

Chairman CHABOT. Thank you. The gentleman yields back.

The gentleman from Pennsylvania, Mr. Evans, who is the Ranking Member of the Subcommittee on Economic Growth, Tax, and Capital Access is recognized for 5 minutes.

Mr. EVANS. Thank you, Mr. Chairman.

I am going to ask these questions and I would like for the whole panel to respond to them.

Are there lessons from counterintelligence and counterterrorism that we can apply in our fight against cyber threats? Although today's hearing is focused on a Chinese company, it is critical that we do not turn a blind eye to other potential hackers from abroad. Are there other countries we should be paying attention to?

Mr. OLSEN. I can start if that is all right.

First, on your first question, Mr. Evans, there certainly are lessons we can learn from the counterterrorism fight from the last 16 years where we have learned—that we can apply to cybersecurity. And I will just list them quickly. One, is it a team effort? We need to work together. The government needs to work in cooperative fashion across the government, but in particular, the government and the private sector need to work very closely together because 98 percent of the nation's critical infrastructure are in the hands of the private sector, which is the primary target for cyberattacks. It is a team effort.

Two, we need to build up a cadre of cyber expertise. We did that in counterterrorism. I worked with them at the National Counterterrorism Center, a lot of experts. We need to do the same thing in cyber. We have a dearth of cybersecurity expertise in this country that needs to be filled.

And third, we need to harden our defenses. Again, we did that with respect to terrorism. We put a lot of money and resources into hardening our defenses. We need to do the same thing in cybersecurity. So those are the lessons I think we can learn.

In terms of other countries that pose a significant threat, I think typically I would consider four significant countries that pose a threat. They include certainly China, but also Russia, Iran, and North Korea.

Mr. LINGER. I will chime in. Clearly, plenty of bad actors. The key is to go ahead and get your defenses in place. And for small companies, a lot of low-hanging fruit for them to get up to a 90 percent level of protection versus being in the twenties or zero percent.

Therefore, with regard to who the bad actor is, you are going to be protected. So that is the first step.

Mr. KEISER. It is a great point, Congressman. So certainly, the Chinese are most aggressive in particularly theft of intellectual property here in the U.S., but others have launched very devastating attacks. I mean, the North Koreans almost took Sony off the map. Some experts believe if they were a U.S.-based company, they would not exist anymore after that attack. It was so devastating. The Iranians, of course, went after our financial system in New York in a meaningful way, so plenty of bad folks to keep an eye on.

Mr. EVANS. In terms of lessons would you say to the question I asked, applying fighting, any lessons?

Mr. KEISER. Well, it is important to understand the infrastructure of the internet, I think, to understand the threat. The internet was not built for security. The internet was built for ease of communication. So there is a fundamental flaw that Matt and his colleagues, certainly his old colleagues at the NSA, grapple with every day which is exactly that. So obviously, hardening the systems. A general awareness. I mean, the majority of the attacks still are very low level, simple phishing attacks or other things that could be prevented with a little cyber hygiene we call it in the business. So really the whole country rallying around those sort of simple tasks would have a meaningful impact.

Mr. EVANS. Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman CHABOT. Thank you. The gentleman yields back.

The gentlelady from American Samoa, Mrs. Radewagen, who is the Chairman of the Subcommittee on Health and Technology is recognized for 5 minutes.

Mrs. RADEWAGEN. Talofa. Good morning.

I want to thank Chairman Chabot and Ranking Member Velázquez for holding this very important hearing. And thank all of you for testifying.

Though this hearing is about the threat of ZTE to America's small businesses, make no mistake. It is not just ZTE extending their tentacles around the world as Mr. Keiser said, this is about the tactics that the Chinese state is using to subvert democracy abroad.

My own home district of American Samoa is just next door to, or 40 miles from independent Samoa. The Chinese state has heavily invested there, so much so that they are building a port where vessels of the Peoples Liberation Army and Navy can make call. As Chairman of the Subcommittee on Health and Technology, I take this threat seriously.

Gentlemen, what actions can we take to protect small businesses from unfair competitive practices of Chinese firms?

Mr. OLSEN. I suspect that we all have some thoughts about that. So thank you for that question.

I do think, as you pointed out at the outset of your comments that we do see that China has become increasingly aggressive in the region, and particularly in the South China Sea. And we have also, I would say, from a cyber perspective, that cyber has become a vector of attack that China uses or could use to advance its na-

tional interest. What we have seen historically from China as Mr. Keiser pointed out is using cyberattacks or cyber espionage as a way to gain competitive advantage. That is to steal information, intellectual property from American companies.

In answer to your question directly, I would say that there are, and again, Mr. Linger talked about this, but there are so many things that small businesses can do that we would put in the category of low-hanging fruit, that is, hardening their capacity to withstand a cyberattack by improving their defenses. And then relatedly, to improve their resilience. That is, to be in a position to better respond because to a certain degree, cyberattacks are inevitable. So how a company responds, how quickly it responds, how it responds from a strategic communication standpoint, those often have a lot to do with how effective they are in withstanding a cyberattack.

Mrs. RADEWAGEN. Mr. Keiser?

Mr. KEISER. Sure. Thank you for the question.

So Matt got into the details on the defensive side. A couple important things have happened in recent years. Under the Obama administration, they first issued indictments of Chinese PLA officers, Peoples Liberation Army officers who were involved in the actual theft of American intellectual property which sent, of course, you are never going to get them in a U.S. court, but it sent a pretty important signal that we are not just going to sit back and tolerate that.

Other actions have identified some of these actors, including a private sector report called a Mandiant Report, which I would commend to everyone's reading that specifically named the PLA offices in China, where they were, what they were doing in this aggressive activity. It got folks' attention. Actually, took them off the map for a handful of months. They, of course, rebranded and went back to their old ways. But nonetheless, actions like that, I think, are important. I think this ZTE action is very significant. I mean, you took a top five telecommunications company in the world off the map. Now we might throw them a lifeline here, but Congress I think is going to have the last say on that. I think some of us up here are hoping anyway.

Mr. LINGER. Yes. Thank you for the question. I think Mr. Olsen hit the nail on the head. It is in the planning. Doing your planning for cyberattack just as though you are planning your company's budget for the year or your annual strategic planning. It is something you just have to do. Be diligent on it. Having a plan in place so that if an attack occurs you know how to respond to it.

Mrs. RADEWAGEN. Thank you, Mr. Chairman. I yield back.

Chairman CHABOT. Thank you very much. The gentlelady yields back. The gentlelady from North Carolina, Ms. Adams, who is the Ranking Member of the Subcommittee on Investigations, Oversight, and Regulations is recognized for 5 minutes.

Mrs. ADAMS. Thank you, Mr. Chairman. Thank you, Madam Ranking Member.

If I could just take a moment and introduce three students who are interning, Jemia Booker, North Carolina. All from Carolina, let me say. Jemia is from JCSU in my district. Jasmine Caruthers,

South Carolina, CBC intern. And Tony Watlington from North Carolina A&T where I went to school.

But let me thank all of you for your testimony. This is a very interesting discussion. The back and forth between President Trump and China on tariffs has been incredibly concerning for my state of North Carolina. Many of the products targeted by China's retaliatory tariffs are major exports from my state. A large part of Trump's stated reasoning for initiating this potential trade war with China was the intellectual property policies, but a deal on ZTE now seems to be a key part of these negotiations. Are these tariff negotiations and the deal on ZTE announced by the Commerce Department sufficiently effective in protecting American companies from the cyber threats posed by ZTE and other Chinese companies? This question is for Mr. Olsen.

Mr. OLSEN. I do think that when we talk about the cyber threats from China, a multi-pronged approach is the right one. So we have talked about many of the features of such an approach which include obviously the hardening of our defenses, you know, improving our cybersecurity across the board. A key part of that, and Congress can play a role here is in promoting information sharing between companies, among companies in a sector, as well as between the government and private industry. And Congress has played a critical role in promoting such information sharing. So that is one piece of it.

I do think that taking a strong stand against China, whether that is through, for example, what Mr. Keiser talked about, the prosecution of Chinese government hackers. That did seem to have an impact. That was an aggressive step by the Department of Justice, and I think that was the right thing to do. I think we should demand that where we see that type of activity by China, that the criminal justice system is quite effective or can be quite effective in sending a deterrent message.

But I think when you talk specifically about ZTE or Huawei, that the steps that the Commerce Department took both in sanctioning ZTE and also in imposing additional fines for being deceptive, that is exactly the right thing to do. And as a former prosecutor, I speak I think with some degree of understanding how important it is when a company during the course of negotiations is deceptive and lies to the government, then you cannot allow that to go forward.

Ms. ADAMS. Thank you.

You know, one of the challenges for small businesses in the space is the cost of implementing a cybersecurity plan. Unfortunately, we know that minority-owned small businesses are more likely to face obstacles like difficulty accessing capital. How can Congress ensure that we are inclusive of minority-owned and disadvantaged small businesses and any policies that we implement to encourage small businesses to invest in cyber security?

Mr. Olsen?

Mr. OLSEN. You know, investment in cybersecurity is a challenge across the board. I think Mr. Linger talked about how it needs to be part of the risk management and strategic plan for every company. And it is very hard in particular for small companies who have so many demands on their limited resources to take the steps necessary to invest in security, particularly cybersecurity,

because the risk is not well understood and the really sobering fact is that even our biggest and strongest companies are really no match for a nation state. A determined nation state. So I think that the challenge is one that companies face across the board.

Ms. ADAMS. Thank you.

Mr. Linger, let me quickly ask you about common mistakes that small businesses make in their approach to cybersecurity and how they can be avoided.

You have got about 36 seconds.

Mr. LINGER. Sure. Thank you. It is just doing the basics. Just having a strong password policy across the company. Protecting their servers. Some of these companies, they are small and they really need to put up about $50,000 down on hardware and software and continuous monitoring of their systems to be protected. They have got to try to plan for this. But that is the issue. Some of it can be done internally with policy, but a lot of it does require some technology and monitoring.

Ms. ADAMS. Thank you very much.

Mr. Chair, I yield back.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentleman from Utah, Mr. Curtis, is recognized for 5 minutes.

Mr. CURTIS. Thank you, Mr. Chairman and Ranking Member. This is a really important hearing, and I am grateful that you have put this together, and I appreciate our witnesses that have come to be part of this.

Over the last several years, and particularly the last few months, we have witnessed foreign actors taking steps to infiltrate America's infrastructure and weaken our national security. Utah, where I am from, is a great state of innovation and nationally recognized for our tech community. And it has been instrumental in the great economic development the tech community has in our state. However, with all these impressive innovations comes risks.

More than ever before, criminals are targeting our computer networks and technology infrastructure, instilling proprietary information. In fact, Utah state government's own network sees an average of 5 million attacks every month. Small businesses are not immune from cyberattacks, and as we have heard here today, are actually more likely to be targeted because they lack the resources.

As a former small business owner, I understand that many small businesses do not have an IT department. Mr. Linger, I hear you say $50,000, and that is just insurmountable for many small businesses. As a matter of fact, usually the owner or the family members take that IT hat and try to deal with this problem. Because of this, I am proud to cosponsor and be a supporter of the Chairman's Small Business Cybersecurity Enhancement bill that will give small businesses better access to defense measures to defend against cyberattacks.

So my question for the three of you is what is the very most important thing that we can be doing to help these small businesses here in Congress, protect them from the bad actors, like ZTE and others?

Mr. Linger, let's start with you.

Mr. LINGER. Any support that you can provide for those small businesses, it is so critical. I mean, it is a significant investment that they do not have. And to your point, oftentimes, their IT department is the owner's son who is in high school; right? You see that again and again. Yes. So any measure that can flow down to help them with those systems is imperative.

Mr. KEISER. A couple things that have not been mentioned Mr. Olsen touched on. Information sharing. So Congress did pass a law a couple of years ago to encourage classified threat information to be shared mainly with the ISPs, the internet service providers, that would essentially patch known vulnerabilities so the small business owners would be the beneficiary of that but, of course, might never see it because it would happen upstream. So that is one.

Another impotent one that Congresswoman Adams mentioned is the educational component. So training the next generation of sort of cyber warriors. And they do not always need a 4 or 8-year computer science degree but maybe a 2-year degree in just understanding the basic blocking and tackling of cybersecurity is another area I think that Congress could look at.

Mr. CURTIS. Thank you.

Mr. OLSEN. And I do think picking up on that last point that the Committee has been active in promoting education and training for cybersecurity for small businesses, I think that is critical. That is one.

I think two is the promotion and development of standards so that companies have a sense of what right looks like in this space. What does it look like? What is achievable? And doing so with a particular sensitivity and eye toward the challenges that small businesses face as opposed to Fortune 100 companies.

And then third, moving more broadly, I do think that there is an opportunity in the market for cybersecurity companies to help smaller companies pool together so that they are not in this alone. So what cybersecurity is today is largely you are on your own. Every company is doing this by themselves. The ability of companies to work together to share information, threat information without fear of liability or spilling proprietary information, there is a movement afoot to do that, and the more companies can pool their resources and work together in a common defense, the more effective they will be.

Mr. CURTIS. So it is interesting. As you were all three talking I was thinking to myself, is there a role for a chamber of commerce or somebody like that who historically has worked together with health plans and things like that. Are you seeing that take shape? And is there any way that we could nudge that forward that you can all think of?

Mr. KEISER. So every major industry has something called an ISAC, information security sharing, that does exactly that. So probably the furthest along would be the financial services sector given the type of information they hold and the value. But every sector is coming up with these ISACs. So you even have a health ISAC. You have energy. And others are coming online. I think the more, the better. As Matt said, it is a huge ecosystem and you have to patch all of it at the same time to have complete security that we likely will never be able to achieve.

Mr. CURTIS. Thank you. I would love to hear more. I am afraid I am out of time. And so thanks once again for coming and holding this hearing. And I yield my time.

Chairman CHABOT. Thank you very much. The gentleman yields back. The gentleman from Florida, Mr. Lawson, who is the Ranking Member on the Subcommittee on Health and Technology is recognized for 5 minutes.

Mr. LAWSON. Thank you very much, Mr. Chairman. And welcome to the Committee.

I was just listening to most of your testimony and I was wondering if there was any question I could ask you. And the reason being is that I see small business kind of like three levels. I was a small business owner myself. One from up to 100,000, one to a quarter of a million, and the ones to a million. So you leave a wide gap in there. There is a wide gap in there among these businesses. And I was just trying to think from your standpoint hearing the testimony this morning, I guess it is after noon now, and the question may be more appropriate for the Justice Department. But what modification at the Federal level can be made to protect a cyber system from hacking from companies like ZTE? You know, and maybe you might want to comment on that because, you know, at some of the levels I dealt with, they do not know anything about cybersecurity. All they know is something happened to them, you know, so what can the Federal government do?

Mr. OLSEN. It is a great question because, you know, much of the risk is borne by the private sector at the local level, small companies that are really being hit on a daily basis with relatively small scale cyberattacks. Whether it is a ransomware, someone who locks up your data, stealing of data. So these can be devastating but they do not rise to the level of a national security threat perhaps or at least in the isolated incident.

But there is a critical role for the Federal government to play on a number of levels. One, as we are talking about today, when we identify a bad actor like ZTE, to use the tools that the Federal government has, whether those are the tools of prosecution, regulatory, sanction-related tools, like the Commerce Department and the State Department have, you know, to use those tools and to use them directly when we have a bad actor that we have identified, and that is really the case with ZTE. But from a policy level more broadly, both Mr. Keiser and I have spoken about Congress's Enactment of the Cyber Information Sharing Act of 2015. What that act did was to really address some of the concerns that companies had about liability perhaps or anti-trust concerns about sharing cyber threat information and it eliminated those. So it addressed those and took those away. And that, as I have talked a little bit about, you know, the ability of especially large companies to get together and to act in a common dense, just like a neighborhood watch, for example, because what these actors do, bad actors are doing is they are going down the line. They do not really care which company they hit. They will just knock on the door until they get in. And so if you are only acting by yourself, you know, you are vulnerable. But if companies share information, if they see something they can share that quickly in a way that can protect them, then they are going to be much better protected, and Con-

gress can play a real important role from a policy perspective in encouraging that.

Mr. LAWSON. Mr. Keiser?

Mr. KEISER. One thing to think about, I think there are, as you mentioned, the different size companies is an important point. You have some small firms that are huge targets for espionage, particularly law firms, tax firms, that might be small and fit those small categories you mentioned, but hold awfully important information. I mean, we have seen cases of the Chinese getting into a law firm, stealing their information because they were active in a bid or in a merger and acquisition and they wanted that information to use to undercut the bid. So you see different aspects of that.

There is a line though in cybersecurity that goes something like this. There are companies that have been hacked by the Chinese and know it, and then there are companies that have been hacked by the Chinese and do not know it.

Mr. LAWSON. Wow.

Mr. LINGER. Yeah, I will just reiterate. It is that supply chain. So those larger companies are going to have more in terms of protection, but they are going to find the weakest links. Somewhere down the supply chain there is going to be a small manufacturer that makes a critical component that they are very good at producing and those are the ones that are going to be targeted. So sharing that information across that board, supporting those larger companies that give those best practices down to the smaller companies is a way to help make the entire supply chain safe and secure.

Mr. LAWSON. Okay. And I do not have much time but Mr. Olsen, since you have been a prosecutor, are we hacking anybody? I mean, if you do not want to answer I can understand.

Mr. OLSEN. We are not like the Chinese.

Mr. LAWSON. That might have been an unfair question.

With that, Mr. Chairman, I need to yield back.

Chairman CHABOT. Thank you very much. The gentleman yields back.

I think that concludes on both sides. We want to thank our very distinguished panel for being here today. As you know, this Committee is responsible for doing everything it possibly can to help small businesses and to protect them, and they continue to be targets for cyberattacks. And the Ranking Member and I have worked on legislation on this to help to protect. For example, it has the SBICs using best practices out there to educate the small business communities, what they can do to protect themselves. But it is still a dangerous world out there. And as you all mentioned, you have got North Korea, you have got Iran, Russia, and especially China constantly. The gentleman from Utah mentioned 5,000 attacks in his state in one month. So it is incredible what they have to put up with.

So thank you for helping us, and especially drawing attention to ZTE and Huawei and what they have been doing and how our country needs to do everything possible to protect ourselves from them in particular.

And then finally, I just would note, you mentioned Sony and the attack on them. If my recollection serves me I think was that not

in response to a movie? It was, I think, the Interview, Seth Rogan and James Franco? I felt it was my patriotic duty to see the movie, which I did, if for no other reason than to annoy Kim Jung-un. So, but we do appreciate you mentioning that, and I am certainly glad they did survive that because it was a serious attack.

So again, we want to thank you all very much for what you have done to help this Committee to help America's small businesses.

And I would ask unanimous consent that members may have 5 legislative days to submit statements and supporting materials for the record.

Without objection, so ordered.

If there is no further business to come before the Committee, we are adjourned. Thank you.

[Whereupon, at 12:11 p.m., the Committee was adjourned.]

[Mr. David Linger's Response to Questions were not submitted in a timely manner.]

APPENDIX

CONGRESSWOMAN YVETTE D. CLARKE
REPRESENTING NEW YORK'S 9th CONGRESSIONAL DISTRICT

Congresswoman Yvette D. Clarke Statement for the Record
ZTE: A Threat to America's Small Businesses
June 27th, 2018

- Thank you Mr. Chairman and Ranking Member Velazquez.
- China is the world's largest infringer of intellectual property law and one of the biggest participants in cyber espionage.
- Chief among China's cyber espionage culprits are ZTE and Huawei, which have been caught violating international sanctions against Iran and North Korea.
- Yet, despite clear evidence of continued malfeasance from the Department of Commerce, President Trump saw fit to grant ZTE a reprieve and lift sanctions against it on June 7, 2018.
- This is irresponsible and downright dangerous. By refraining from attaching a cost to attacks against American companies and persons, we incentivize further misconduct.
- Furthermore, China's increased efforts to obtain 5G technology make it an ever-powerful security threat, particularly to small businesses which often lack the knowledge and resources to protect themselves.

TechSolve®

STATEMENT FOR THE RECORD OF
DAVID LINGER, PRESIDENT/CEO - TECHSOLVE, INC.

BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
HOUSE SMALL BUSINESS COMMITTEE

REGARDING A HEARING ENTITLED
"ZTE: A THREAT TO AMERICA'S SMALL BUSINESSES"

WEDNESDAY, JUNE 27, 2018

TechSolve

INTRODUCTION

Chairman Chabot, Ranking Member Velázquez, and Members of the Committee, thank you for inviting me to testify on behalf of U.S. small manufacturers regarding the impact of cyber-attacks on this critical national asset. Only the government tops the manufacturing sector (followed by finance and healthcare) as the most targeted sector by cyber espionage. These aggressors are seeking to disrupt manufacturing not only through the espionage of intellectual property; but also the destruction of the U.S. supply chain by crippling them both financially and through attacks on their intelligent machines.

These foreign criminals are exploiting the information that manufacturers believe they've safely locked away. These hackers have proven how private data, on any computer or manufacturing device that is connected to the Internet, is vulnerable and susceptible to malicious attacks, tampering, theft, and misuse. Unfortunately, it is not an exaggeration that there are only two types of companies - those who have been hacked and those who don't know that they have been hacked. "Most manufacturing systems today were made to be productive - they were not made to be secure. Every manufacturer is at risk - it isn't a matter of if they will be targeted, it's a matter of when." said Rebecca Taylor, senior vice president for the National Center for Manufacturing Sciences (NCMS).

TechSolve has found that a majority of manufacturers can be described as "not very well prepared" or "not prepared at all" to handle cyber-attacks. A 2017 Ohio Manufacturing Extension Partnership (OH MEP) survey of Ohio manufacturers revealed that only 12.51% manufacturers responded that they understand what cybersecurity is and have worked to protect their machines, intellectual property, and IT systems and only 4.48% have undergone a cybersecurity assessment.

THE IMPORTANCE OF SMALL MANUFACTURERS

According to 2015 Census data, the vast majority of manufacturers are very small. Of the 251,744 firms in the U.S. manufacturing sector, only 1.5% of those manufacturers have greater than 500 employees. And out of the remaining 98.5% of manufacturers with less than 500 employees, 75% of those manufacturers have less than 20 employees. The importance of these 188,000+ very small manufacturers to the United States' economy is staggering. These small firms are the backbone of manufacturing - the ninth largest economy in the world with over $2.1 trillion in value-added.

In addition to their contributions to the economy, creating jobs, and building products critical to our daily life and defense of this nation, small manufacturers are especially important because they drive innovation. Brian Raymond, Director of Innovation Policy for the National Association of Manufacturers (NAM) impeccably

summarized manufacturers' recent digital transformations, and subsequent rising exposure to cyber-attacks in the Fourth Industrial Revolution: "Manufacturers are the creators, users, servicers, and installers of the Internet of Things (IOT). Billions of connected devices are pervasive throughout manufactured products and on the shop floors where they are made. This technology is creating enormous opportunity and driving transformative change. It has made all manufacturers into technology companies. The IOT will increase the attack surface for manufacturers. The more that shop floors become imbued with intelligent machines, the more those machines will contain data worth stealing."

THE CYBERSECURITY CHALLENGES THAT SMALL MANUFACTURERS FACE

Attacks against larger businesses and nations hit the headlines with such regularity that many have become numb to the sheer volume and hastening of cyber threats. These threats are not hypothetical evils. For those of us that work with small manufacturers who have teetered on the brink of closing their doors due to cyber-attacks; their cyber-crimes are personal, real, and distressing. As president of TechSolve, I have a very unique perspective of the devastation these cyber-attacks have caused our customers. I am here today to share the story of one such manufacturing company that has experienced these attacks and exemplifies the risks a majority of these manufacturers face on a 24/7 basis.

To Tony Strobl, President of Cincinnati Crane & Hoist, these cyber-attacks are war on his company and his employees. Cincinnati Crane is a very small, 20-person company, based in Southwest Ohio, that supplies turn-key crane systems, parts, and services, through hard work, innovation, and quality craftsmanship, at competitive prices to a global market. Cincinnati Crane is a veteran-owned business that has seen domestic growth of more than 400% in the last three years and was awarded the U.S. Department of Commerce Export Achievement Award in 2017. Earlier this year, Tony's company was the victim of social engineering, or more specifically a spear phishing campaign that contained malicious macros that breached their email system; went undetected for an uncertain amount of time; embedded hidden folders within Office365®; "spoofed" legitimate invoices that were being emailed to Cincinnati Cranes' customers; replaced those invoices with bogus invoices providing illegitimate banking information that ultimately syphoned over $200,000 from his customers. When the Cincinnati Crane invoices had aged 30 days and collection calls were made, customer after customer told Cincinnati Crane that they had already paid their invoices.

The $200,000 that was stolen from Cincinnati Crane is unrecoverable according to the FBI. Due to Cincinnati Crane's current financial standing, Tony had to make the devastating decision to lay off four of his employees - 20% of his company. Not only has this cyber war devastated the lives of those four families; but it has also

severely hampered Tony's capability to complete customer orders, grow, and innovate. This cyber-attack has also resulted in a devastating fluctuation in customer trust. Cincinnati Crane's customers are afraid to conduct business with Tony. Not only are they concerned about sensitive drawings and corporate data that they have shared with Tony's project managers; but they are also afraid to open email correspondence from Cincinnati Crane or make payments to him electronically. Even though TechSolve, and its IT sub-contractors, have scrubbed their systems and are working on long-term cybersecurity policies and procedures through remediation and adaptation of the NIST SP 800-171 cybersecurity controls, the effects of these cyber-attacks continue to devastate his company and threaten its long-term viability.

Customers, like Cincinnati Crane's, share their sensitive information with manufacturers, assuming these companies have the proper security measures in place to protect their data. As soon as a data breach occurs, customers will question the amount of trust they've put into that business. Furthermore, these customers want to believe that the manufacturer can not only prevent; but also properly manage a potential data breach. While the cyber-hack itself might affect customer loyalty, manufacturers that don't handle the attack with competence will likely see a more negative impact on customer confidence. Obviously, the majority of customers won't do business with a manufacturer they can't depend on and when it comes to a large prime or the Department of Defense (DoD), these manufacturers probably should expect to lose their government contract. Government primes already have a difficult time finding and maintaining quality suppliers.

Besides typical IT cyber-attacks, both foreign and domestic espionage will continue to target manufacturers and devastate these companies, and their customers and supply chain primes, because there is fierce competition for intellectual property; industrial control systems (ICS) that are largely left unguarded; and their systems are increasingly connected through the use of IOT devices, robotics, and human-machine interfaces to improve automation and decrease costs.

In 2018, reports released by highly-respected American corporations Symantec Corporation, NTT Security, and Cisco Systems validated data that TechSolve has encountered when working with small manufacturers. The four biggest obstacles to adopting advanced security processes and technologies in small U.S. manufacturers are: 1) Budget constraints; 2) Competing priorities - focus on productivity and efficiency; 3) Lack of knowledge regarding the invasiveness and impact of cyber-attacks; and 4) Defense contractors choosing the calculated risk of not implementing and/or slow cybersecurity remediation since (to date) there is a lack of enforcement of the current DFARS SUBPART 204.73--SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (Revised December 28, 2017).

The Cisco 2018 Security Capabilities Benchmark Study further corroborates data TechSolve has observed when it comes to manufacturers in general; but especially small manufacturers. There will be more operational technology (OT) and IOT attacks in the future. Attacks targeting OT are still classified as "uncommon" enough that many cybersecurity professionals haven't experienced them firsthand. But in Cisco's study, security professionals absolutely agree that manufacturers should expect such attacks to occur in the future. Since TechSolve has 35+ years' experience in serving the needs of manufacturers in the areas of machining, data extraction, and manufacturing process improvement, we are used to working with small manufacturers every day to translate emerging technologies into everyday manufacturing and business solutions. TechSolve is currently working on solutions for manufacturers that will help them "connect and protect" their systems that, a majority of the time, have unpatched and out-of-date software making them even more vulnerable to cyber-attacks. Many manufacturers have older OT devices and equipment that use controllers based on Microsoft Windows XP®, and even MS DOS, that are connected to the Internet; therefore their risk of cyber-attacks is exacerbated. Some other manufacturers have fabrication presses, machine tools, and material handling equipment that are 25, 30, or even 40+ years old. Manufacturers don't get rid of these items just because they aren't the "latest and greatest"; but are working to connect the analog control of this equipment to the digital thread via the Internet. The Industrial Internet of Things (IIOT) will be pervasive and therefore, the need to protect is vital.

Similar cyber-attack opportunities also exist for "disruption of operation" attacks and hardware attacks. Cyber-attackers can hack into machine tool accessories or machine tools and adjust/alter the program; therefore either stopping the manufacturer from providing the right parts for their suppliers, or even worse; altering the quality of the part that is a portion of a larger assembly, thus compromising the entire system. For large defense primes and original equipment manufacturers (OEMs), it is critical for their supply chains to protect what happens to their parts before they enter back into their network.

HOW CYBERSECURITY REGULATIONS & PROGRAMS AFFECT SMALL MANUFACTURERS

Today, companies like Cincinnati Crane & Hoist have DFARS regulations to which they must comply in order to keep their government contracts. However, the spirit of these regulations may have the safety of our nation at heart; but the government's lack of enforcement make Cincinnati Crane's systems and critical information no safer by merely becoming "compliant" with DFARS.

Safeguarding data is too important to the United States to allow "loose compliance" to be the platinum standard. There are a number of ways to entice

companies to begin implementing cybersecurity best practices and the DoD has done a great job by leading the way and establishing one method - regulation through the current DFARS and NIST SP 800-171 controls. The current shortcoming of this exercise is the lack of enforcement. TechSolve is working with several manufacturing companies that are conducting business with the DoD. They are technically "in compliance" with the DFARS by completing all four of these items: 1) conducting a cybersecurity assessment; 2) creating a security plan based on the assessment; 3) creating a plan of action with milestones (POAMs) based on the work that needs to be done in the security plan; and 4) creating an incident response plan (IRP) that will report designated security breaches within 72 hours of the incident; however they are not automatically cybersecure. These documents, without remediation of the weaknesses in their systems, are merely "pinky swears" to make their networks safer at some future date. A plan of action is great; however, there are no existing checks and balance system that is currently being implemented by the DoD to manage these POAMs.

Another approach is being discussed in the state of Ohio. Attorney General Mike DeWine is working with the Senate and House on former Senate Bill 220. This "safe harbor" legislation, if passed, will create a law that will protect companies that can prove that they have proactively implemented and are maintaining cybersecurity measures within their systems. If these Ohio companies can document that they have taken steps to safeguard the information on their networks, they will have a limited amount of protection from civil litigation.

Although both of these examples have different goals; the methods in both cases are implementation of cybersecurity best practices. While cybersecurity is not a solution to being hacked, it does make it much more difficult for these cyber-criminals to devastate our nation's small manufacturers. Research conducted by the National Cyber Security Alliance states that there was a 600% increase in IOT attacks from 2016 to 2017 and that the #1 country of origin is China at 21% while the next highest country of origin is 10.6%. Given these statistics and the fact that 60% of small and mid-sized businesses that have been hacked have to shut down within 6 months of a cyber-attack, it will be important for the U.S. government to be aware that it must have more concrete plans in place to safeguard this incredibly important industry sector.

Andy Keiser
Visiting Fellow, National Security Institute
George Mason University's Antonin Scalia Law School

Testimony before the United States House Committee on Small Business
June 27, 2018 hearing titled: ZTE: A Threat to America's Small Businesses

Thank you Chairman Chabot, Ranking Member Velazquez and distinguished members of the Committee.

As someone who spent the first part of my career roaming these halls as a House staffer, it's wonderful to be back home among friends – particularly before a Committee that is taking a sobering, bipartisan look at one of America's greatest long-term national security threats: the threat posed by Zhongxing Telecommunications Equipment Corporation (ZTE) and Huawei to our telecommunications infrastructure.

I will start with a story to which I imagine many of you will easily relate. My former boss, House Intelligence Committee Chairman Mike Rogers, first became interested in the activities of ZTE and Huawei not because he was a former U.S. Army officer or Federal Bureau of Investigation (FBI) special agent. Initially, his interest did not even stem from his position on the Intelligence Committee, but because a Michigan company approached him with a problem.

As each of you would do, he listened to that small business owner carefully. As it turned out, Chinese telecommunications companies –ZTE and Huawei – were bidding to build cellular telephone towers in the most rural parts of Michigan, far from population centers like Detroit. This small business owner was happy to compete but said the Chinese telecoms were coming in not just under his price, but under what *the materials would cost* to build the towers.

That got a former FBI agent thinking: why on earth would they be doing that? More on this later.

As I don't need to remind this room, small business is the lifeblood of the American economy. Small business employs more than half of the U.S. workforce and two out of every three new private-sector jobs created in America are created by small businesses.

Small business in America is inherently resilient, creative, and able to adapt quickly to market conditions. One thing small business cannot do effectively, however, is compete against nation-state attacks, aggressive, unrelenting international espionage, and theft of trade secrets. And those are exactly the challenges presented by ZTE and Huawei.

For thousands of years, China viewed itself as superior to all other world powers. Following a self-described "century of humiliation" resulting from imperialist incursions from the West and Japan, it now seeks a return to that perch.

Under the consolidated leadership of Xi Jinping, newly declared "President for life," China today intends to become a global economic, military and technological leader rivaling or surpassing the United States and it aims to do so in the next 10-15 years. There are troubling indicators: China's gross domestic product is currently on track to surpass that of the United States by 2029. And the Chinese military is rapidly modernizing, directly targeting areas in which the U.S. maintains dominance, including in the cyber domain, space and power projection at sea.

When I attended the Shanghai-hosted World's Fair in 2010, China was portrayed as a civilization that led the world for millennia. The storyline went that, now with failing powers like Russia and stagnating powers like the United States and Europe, China will again be called upon to lead the way into the future.

Part of China's grand vision includes dominance in fields that have dual economic and military benefit. In 2015, Chinese leaders unveiled the "Made in China 2025" strategic plan. It focuses on the country becoming the world's leader in high-tech fields, squarely within the learned and stolen expertise of ZTE and Huawei.

ZTE and Huawei are working fast to put Western vendors out of businesses to secure market dominance. In just seven years, Huawei went from an afterthought with poorly-functioning equipment and only 10 percent market share to having the top position now in the lucrative LTE radio business. Excluding the United States, Huawei enjoys roughly 38 percent of the total market share globally.

By investing heavily in research and development, ZTE and Huawei are organically improving their native capacity to innovate, but they also have copied and stolen their way to success. Huawei has admitted to stealing router product secrets from Cisco. The theft was extensive, all the way down to the spelling errors in the manuals. And apparently Huawei stole the design for Apple's iPhone literally down to the last screw.

Nonetheless, Huawei has surpassed every telecommunications provider in the Asia Pacific, Europe and in Latin America. Only markets in the United States and Middle East remain competitive due to the concerns raised by vocal U.S. government security leaders in the Administration and Congress. Huawei is now dominant in fixed access, IP routing, and LTE in many markets and is growing shares of these critical businesses in others. Western vendors are still able to compete for certain products and in certain markets, but it is unclear how long that will remain true. Absent U.S. government initiative and continued attention, the only telecommunications infrastructure option available in the world in the not-too-distant future could be a Chinese one.

In my view, ZTE and Huawei do not share the motivation of most Western companies. Profit is not the motive. Deploying equipment in rural Michigan and all around the world at or below cost is not being done to make shareholders money; it is being done to harness the ability to collect vast quantities of information and to create leverage against adversaries in a potential conflict. National security thought leaders from both parties - like Senators Marco Rubio and Mark Warner – have brought attention to this threat. If Chinese telecom giants are allowed to infiltrate our telecommunications backbone, in a potential conflict they could incapacitate critical infrastructure – for instance, our electric grid — bogging us down at home, while impairing our capacity to respond overseas.

Chinese companies generally cannot be decoupled from the Chinese state. Resident Scholar Derek Scissors with the American Enterprise Institute has said, "ZTE is a tool of the Chinese state, which is controlled by the party." Indeed, under Chinese law, all Chinese companies, including Huawei and ZTE, are required to fully cooperate with Chinese law enforcement and intelligence services.

If there was any question about Chinese government support to ZTE and Huawei, consider that ZTE is currently working to secure an $11 billion financing package from the Bank of China and the China Development Bank. This was done after losing nearly half of its' value following the issuance of the U.S.

Commerce Department's denial order forbidding their acquisition of U.S. components. It is fair to say that no Western supplier would be able to secure that level of state-sponsored cash infusion under such circumstances.

ZTE and Huawei have developed dubious reputations around the world. In the past 12 years alone, ZTE and/or Huawei entities have been investigated or found guilty of corruption in Kyrgyzstan, Uganda, Cameroon, Ethiopia, Gabon, Zimbabwe, Nigeria, the Philippines, Gambia, Ghana, Algeria, Malaysia, Norway, Zambia, Singapore, South Sudan, South Africa, Papua New Guinea, Mongolia, the Solomon Islands and even in China itself.

The Arab spring led despots and dictators around the world to look to prevent a similar fate to that of Muammar Gaddafi being dragged through the streets. Andrew Rizzardi from Freedom House says the Chinese – i.e. ZTE and Huawei – own the "authoritarian telecommunications hardware store." ZTE and Huawei technologies are being used to suppress dissent in nearly all African countries. In recent years, advanced monitoring technology has been sold to Zambia, Ethiopia, Iran, Pakistan, and Venezuela by ZTE or Huawei. Authoritarianism is now officially a key Chinese export.

The most comprehensive review to date of the threat generated by ZTE and Huawei was conducted right here by the United States Congress in a bipartisan way – specifically, in 2012 by the House Permanent Select Committee on Intelligence (HPSCI). I was Chief of Staff to Committee Chairman Mike Rogers at the time and the report was fully supported by Ranking Member Dutch Ruppersberger. Many of its findings still hold true today.

The 2012 HPSCI report stated that: "the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national security interests."

Most relevant to today's hearing, the report also found that: "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."

As background, ZTE has its origins in the Chinese Ministry of Aerospace and the government-run 691 factory, which is a now part of a state-owned research institution. According to the HPSCI report, the Zhongxinxin group, owned in part by two state-owned enterprises, has a controlling interest in ZTE.

Internal Chinese Communist Party committees are also embedded within Huawei and ZTE. As of 2012, ZTE had Communist Party Committee members on its Board of Directors and serving as key shareholders.

During the HPSCI investigation, ZTE repeatedly argued that it could not provide internal documentation or fully answer the Committee's questions for fear that it would be in violation of China's state secrets law and could be subject to criminal prosecution in China. In my view, this lack of response proves the point of concern.

The founder of Huawei, Ren Zhengfei, was a director of the People's Liberation Army (PLA) Information Engineering Academy, which is associated with 3PLA, China's signals intelligence division and the country's version of the National Security Agency. Ren also retains veto power over the company's decisions.

According to the HPSCI report: "Huawei operates in what Beijing explicitly refers to as one of seven "strategic sectors." Those are considered as core to the national and security interests of the state. In these sectors, the Chinese Communist Party ensures that "national champions" dominate through a combination of market protectionism, cheap loans, tax and subsidy programs and diplomatic support in the case of offshore markets."

A separate, major U.S. investigation into ZTE began in 2012 after Reuters reported on the firm's business dealings with Iran. The Department of Justice found that ZTE conspired to evade Iran sanctions to secure contracts worth hundreds of millions of dollars by installing telecom equipment that required U.S. components, which was in direct violation of U.S. export controls.

ZTE admitted committing 380 violations and engaged in an elaborate scheme to prevent disclosure to the U.S. government, including forming a group to destroy, remove and sanitize all evidence relating to its dealings with Iran.

After failing to comply with the terms of the settlement, the U.S. Department of Commerce issued an April 15, 2018 denial order stating that ZTE demonstrated "a pattern of deception, false statements, and repeated violations."

The denial order forbidding ZTE from acquiring U.S. components went on to state that: "ZTE agreed to a record-high combined civil and criminal penalty of $1.9 billion, after engaging in a multi-year conspiracy to violate the U.S. trade embargo against Iran to obtain contracts to supply, build, operate and maintain telecommunications networks in Iran using U.S.-origin equipment, and also illegally shipping telecommunications equipment to North Korea."

Also, in April, Federal Communications Commission (FCC) Chairman Ajit Pai circulated a proposal to ban Huawei and ZTE from receiving government funds that subsidize low-income Americans' access to phone and internet service.

In a statement, Chairman Pai wrote that: "Hidden 'back doors' to our networks in routers, switches—and virtually any other type of telecommunications equipment—can provide an avenue for hostile governments to inject viruses, launch denial-of-service attacks, steal data, and more."

In a 92-page submission responding to the FCC, Huawei attempted to equate PLA-founded Chinese telecommunications companies with U.S. companies who have a manufacturing presence in China. This is a ludicrous comparison as the U.S. companies are there due to requirements of doing business in China, not out of any allegiance to the Chinese government. The response, carefully written by American lawyers at two leading Washington, DC law firms, parses language from the Directors of the FBI and the National Security Agency in an effort to minimize the threat. It also attributes numerous Constitutional rights afforded to Huawei's U.S. subsidiary. I doubt that the founding fathers of the United States intended to protect the rights of companies controlled by our adversaries seeking to compromise core national security interests.

In response to the ongoing and known security threats by these two companies, last month the Department of Defense ordered all ZTE and Huawei equipment to be removed from military installations.

ZTE and Huawei have the capability, clout, motive and growth strategy to pose a continuing national security threat to the United States – one that directly harms American small business. Surely in part due to your steady work in this committee raising the profile of the issue, Congress has become convinced of this in a bipartisan way.

The legislative House and Senate activity occurring around the 2019 National Defense Authorization Act could provide a long-term solution to the threat posed to the U.S. by reinstating the Commerce Department's denial order forbidding ZTE from using U.S. components, perhaps except for providing common-sense security patching and upgrades. This would be a severe blow to ZTE and would be a critical win for the United States of America's national security posture as we confront a rising China threatening our interests around the globe.

Chairman Rogers and Congressman Ruppersberger again teamed up to pen an Op-ed earlier this year in the *Wall Street Journal* which called the threat from ZTE "a clear and present danger to U.S. national security." I agree completely and encourage this body to respond accordingly.

Chairman Chabot and Ranking Member Velasquez, thank you so much for convening this hearing and raising these important issues. I look forward to your questions.

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.

Questions for the Record
Committee on Small Business
Hearing: ZTE: A Threat to America's Small Businesses
June 27, 2018

Congresswoman Murphy

The 2012 HPSCI report on "U.S. National Security Issues Posed by Chinese Telecommunication Companies Huawei and ZTE" recommended that "U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts. Similarly, government contractors--particularly those working on contracts for sensitive U.S. programs--should exclude ZTE or Huawei equipment in their systems." And as you know, there is consensus within the larger national security community about the security risks of both ZTE and Huawei products. Recently, the Senate and House Armed Services Committees included provisions in their respective versions of the FY 19 NDAA that would bar new procurement and the continued use of existing equipment from these companies in federal government networks and contractor networks.

In your view, is there a material difference for small businesses trying to protect themselves against cyber risks between technology coming from ZTE and technology coming from Huawei?

Response: *No, from my perspective, both ZTE and Huawei present similar levels of cyber risks to our small business community. The risks associated with ZTE and Huawei are well-documented. As the House Intelligence Committee concluded in its authoritative report: "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."*

More recently, the U.S. intelligence community reaffirmed the risks that ZTE and Huawei pose 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."

Congresswoman Clarke

How can small businesses be vigilant of which companies are producing the components of the technology they are using and why does this matter? When learning that ZTE defied U.S. sanctions by shipping equipment to Iran and North Korea, the administration initially banned

ZTE from buying American products, which virtually put the company out of business. It has since lifted the ban and levied harsh fines. How have these fines impacted ZTE's reliance on the United States and are small businesses more at risk with companies like ZTE operating domestically?

Follow-up: Do such financial penalties impact the cyber security risks ZTE poses to businesses in the U.S.?

Response: *In my view, the lifting of sanctions against ZTE has not diminished the national security risks that ZTE poses to the United States and to the small business community. As I stated in my testimony, the concerns regarding ZTE are multifold: First, as the House Intelligence Committee observed, 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, there is the concern about 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 House Intelligence 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."*

Indeed, we have seen bipartisan opposition in Congress to the decision to lift the sanctions and reach a settlement with ZTE, which is now able to business with U.S. businesses.

○