

TELECOMMUNICATIONS, GLOBAL COMPETITIVENESS, AND NATIONAL SECURITY

HEARING BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MAY 16, 2018

Serial No. 115–128



Printed for the use of the Committee on Energy and Commerce
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

32–796 PDF

WASHINGTON : 2018

COMMITTEE ON ENERGY AND COMMERCE

GREG WALDEN, Oregon

Chairman

JOE BARTON, Texas	FRANK PALLONE, JR., New Jersey
<i>Vice Chairman</i>	<i>Ranking Member</i>
FRED UPTON, Michigan	BOBBY L. RUSH, Illinois
JOHN SHIMKUS, Illinois	ANNA G. ESHOO, California
MICHAEL C. BURGESS, Texas	ELIOT L. ENGEL, New York
MARSHA BLACKBURN, Tennessee	GENE GREEN, Texas
STEVE SCALISE, Louisiana	DIANA DeGETTE, Colorado
ROBERT E. LATTA, Ohio	MICHAEL F. DOYLE, Pennsylvania
CATHY McMORRIS RODGERS, Washington	JANICE D. SCHAKOWSKY, Illinois
GREGG HARPER, Mississippi	G.K. BUTTERFIELD, North Carolina
LEONARD LANCE, New Jersey	DORIS O. MATSUI, California
BRETT GUTHRIE, Kentucky	KATHY CASTOR, Florida
PETE OLSON, Texas	JOHN P. SARBANES, Maryland
DAVID B. McKINLEY, West Virginia	JERRY McNERNEY, California
ADAM KINZINGER, Illinois	PETER WELCH, Vermont
H. MORGAN GRIFFITH, Virginia	BEN RAY LUJAN, New Mexico
GUS M. BILIRAKIS, Florida	PAUL TONKO, New York
BILL JOHNSON, Ohio	YVETTE D. CLARKE, New York
BILLY LONG, Missouri	DAVID LOEBSACK, Iowa
LARRY BUCSHON, Indiana	KURT SCHRADER, Oregon
BILL FLORES, Texas	JOSEPH P. KENNEDY, III, Massachusetts
SUSAN W. BROOKS, Indiana	TONY CARDENAS, California
MARKWAYNE MULLIN, Oklahoma	RAUL RUIZ, California
RICHARD HUDSON, North Carolina	SCOTT H. PETERS, California
CHRIS COLLINS, New York	DEBBIE DINGELL, Michigan
KEVIN CRAMER, North Dakota	
TIM WALBERG, Michigan	
MIMI WALTERS, California	
RYAN A. COSTELLO, Pennsylvania	
EARL L. "BUDDY" CARTER, Georgia	
JEFF DUNCAN, South Carolina	

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MARSHA BLACKBURN, Tennessee

Chairman

LEONARD LANCE, New Jersey	MICHAEL F. DOYLE, Pennsylvania
<i>Vice Chairman</i>	<i>Ranking Member</i>
JOHN SHIMKUS, Illinois	PETER WELCH, Vermont
STEVE SCALISE, Louisiana	YVETTE D. CLARKE, New York
ROBERT E. LATTA, Ohio	DAVID LOEBSACK, Iowa
BRETT GUTHRIE, Kentucky	RAUL RUIZ, California
PETE OLSON, Texas	DEBBIE DINGELL, Michigan
ADAM KINZINGER, Illinois	BOBBY L. RUSH, Illinois
GUS M. BILIRAKIS, Florida	ANNA G. ESHOO, California
BILL JOHNSON, Ohio	ELIOT L. ENGEL, New York
BILLY LONG, Missouri	G.K. BUTTERFIELD, North Carolina
BILL FLORES, Texas	DORIS O. MATSUI, California
SUSAN W. BROOKS, Tennessee	JERRY McNERNEY, California
CHRIS COLLINS, New York	FRANK PALLONE, JR., New Jersey (<i>ex officio</i>)
KEVIN CRAMER, North Dakota	
MIMI WALTERS, California	
RYAN A. COSTELLO, Pennsylvania	
GREG WALDEN, Oregon (<i>ex officio</i>)	

C O N T E N T S

	Page
Hon. Marsha Blackburn, a Representative in Congress from the State of Tennessee, opening statement	1
Prepared statement	3
Hon. Leonard Lance, a Representative in Congress from the State of New Jersey, opening statement	3
Prepared statement	4
Hon. Yvette D. Clarke, a Representative in Congress from the State of New York, opening statement	4
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	5
Prepared statement	7
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement	8
Prepared statement	9
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, prepared statement	62

WITNESSES

Charles Clancy, Professor of Electrical and Computer Engineering and Director, Hume Center for National Security and Technology, Virginia Tech	11
Prepared statement	13
Answers to submitted questions	105
Samm Sacks, Senior Fellow, Technology Policy Program, Center for Strategic and International Studies	16
Prepared statement	18
Answers to submitted questions	111
Clete D. Johnson, Partner, Wilkinson Barker Knauer, LLP	29
Prepared statement	31
Answers to submitted questions	116

SUBMITTED MATERIAL

Letter of May 16, 2018, from Nicholas J. Pisciotta, Chief Executive Officer, Sicuro Innovations LLC, to Mrs. Blackburn and Mr. Doyle, submitted by Mrs. Blackburn	63
Letter of May 16, 2018, from Michael O’Rielly, Commissioner, Federal Communications Commission, to Mrs. Blackburn and Mr. Doyle, submitted by Mrs. Blackburn	65
Report on behalf of the U.S.-China Economic and Security Review Commission, “Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology,” April 2018, ¹ submitted by Mrs. Blackburn	
Article, “A U.S. Investment Strategy for Defense,” by Andrew P. Hunger, CSIS, submitted by Mrs. Blackburn	68
Article, “Beijing’s Cyber Governance System,” by Samm Sacks, CSIS, submitted by Mrs. Blackburn, submitted by Mrs. Blackburn	74
Article of March 27, 2018, “In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser,” by Drew FitzGerald and Stu Woo, The Wall Street Journal, submitted by Mrs. Blackburn	82

¹ The information has been retained in committee files and also is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108301>.

IV

	Page
Article of January 8, 2018, “Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings,” by Stu Woo, Dan Strumpf, and Betsy Morris, The Wall Street Journal, submitted by Mrs. Blackburn	84
Order issued April 15, 2018, by Richard R. Majauskas, Acting Assistant Secretary of Commerce for Export Enforcement, submitted by Mrs. Blackburn	89
Article of January 12, 2018, “US Army base removes Chinese-made surveillance cameras,” by Max Greenwood, The Hill, submitted by Mr. Long	103

TELECOMMUNICATIONS, GLOBAL COMPETITIVENESS, AND NATIONAL SECURITY

WEDNESDAY, MAY 16, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:00 a.m., in room 2123, Rayburn House Office Building, Hon. Marsha Blackburn (chairman of the subcommittee) presiding.

Members present: Representatives Blackburn, Lance, Shimkus, Latta, Guthrie, Kinzinger, Bilirakis, Johnson, Long, Flores, Brooks, Collins, Walters, Costello, Walden (ex officio), Welch, Clarke, Loeb sack, Ruiz, Dingell, Eshoo, Butterfield, Matsui, and Pallone (ex officio).

Also present: Representative Walberg.

Staff present: Jon Adame, Policy Coordinator, Communications and Technology; Samantha Bopp, Staff Assistant; Daniel Butler, Staff Assistant; Kristine Fargotstein, Detailee, Communications and Technology; Sean Farrell, Professional Staff Member, Communications and Technology; Margaret Tucker Fogarty, Staff Assistant; Adam Fromm, Director of Outreach and Coalitions; Elena Hernandez, Press Secretary; Tim Kurth, Deputy Chief Counsel, Communications and Technology; Lauren McCarty, Counsel, Communications and Technology; Austin Stonebraker, Press Assistant; Evan Viau, Legislative Clerk, Communications and Technology; Everett Winnick, Director of Information Technology; Jeff Carroll, Minority Staff Director; Jennifer Epperson, Minority FCC Detailee; David Goldman, Minority Chief Counsel, Communications and Technology; Tiffany Guarascio, Minority Deputy Staff Director and Chief Health Advisor; Jerry Leverich III, Minority Counsel; Dan Miller, Minority Policy Analyst; Andrew Souvall, Minority Director of Communications, Member Services, and Outreach; and C.J. Young, Minority Press Secretary.

Mrs. BLACKBURN. The Subcommittee on Communications and Technology will now come to order. And I recognize myself 5 minutes for an opening statement.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TENNESSEE

I want to welcome each of you to today's hearing. It is entitled "Telecommunications, Global Competitiveness, and National Security."

Our country's information technology sector is one of the best economic growth engines the world has ever seen. It allows people to communicate, be entrepreneurs, pursue educational opportunities. It fosters a greater efficiency across every single sector of the economy.

As I have said before, information is power, and history makes clear that countries with the best communications have the best advantage. Moreover, our Nation's defense, the men and women in uniform who serve our Nation depend on communications. U.S. military superiority is built upon intelligence, surveillance, and reconnaissance, and the communication of this information to out-manuever potential adversaries.

The purpose of today's hearing is to understand the nexus between telecommunications and national security in the global context. These are issues the subcommittee and the Energy and Commerce Committee more generally understand well.

In 2013, I authored a bill, H.R. 1468, SECURE IT, to promote greater voluntary sharing of cyber threats between the Government and the private sector, as well as among private sector companies. I was pleased that many of the provisions I authored were signed into law in 2015. Additionally, the National Institute of Standards and Technology, or NIST as we term it, has taken great strides to collaborate with the private sector on developing a voluntary framework of cybersecurity best practices.

Last month, NIST published the latest version of its framework to be even more informative and useful to a broader array of stakeholders. In today's world where information literally travels at the speed of light and new innovations are brought to market at a dizzying pace, it is critically important to leverage robust information sharing about threats and vulnerabilities. This should include greater information sharing about the supply chain of hardware and software that make up our communications networks.

When it comes to the supply chain, we must think about it over the long term. We are fully aware of the issues that the President has raised regarding China, Huawei, and ZTE. We are aware that the Commerce Department has serious concerns. These points merit discussion, and it is the reason our hearing is so timely.

The quick and easy route would simply ban foreign vendors of vulnerable hardware and software from accessing our markets, but the marketplace for hardware and software is global, and a hallmark of the communications industry is scale. In time, it will be difficult for our domestic communications providers to obtain their network infrastructure from trusted sources when vulnerable foreign vendors acquire more and more global market share.

What are the implications of all this to our Nation's cybersecurity? What are the implications in the race to 5G? What are the broader implications to our Nation's economy? And most importantly, what are thoughtful solutions to such a complex problem? These are some of the questions for today's hearing that we will seek to address.

[The prepared statement of Mrs. Blackburn follows:]

PREPARED STATEMENT OF HON. MARSHA BLACKBURN

Welcome to today's subcommittee hearing entitled: "Telecommunications, Global Competitiveness, and National Security."

Our country's information technology sector is one of the best economic growth engines the world has ever seen. It allows people to communicate, be entrepreneurs, and pursue educational opportunities; it fosters greater efficiency across every sector of the economy. As I've said before, information is power, and history makes clear that countries with the best communications have a competitive advantage.

Moreover, our Nation's defense—the men and women in uniform who serve our country—depend on communications. U.S. military superiority is built upon intelligence, surveillance, and reconnaissance, and the communication of this information to outmaneuver potential adversaries.

The purpose of today's hearing is to understand the nexus between telecommunications and national security in a global context.

These are issues this subcommittee, and the Energy and Commerce Committee more generally, understand well. In 2013, I authored a bill—H.R. 1468, SECURE IT—to promote greater voluntary sharing of cyber threats between the Government and the private sector, as well as among private sector companies.

I was pleased that many of the provisions I authored were signed into law in 2015.

Additionally, the National Institute of Standards and Technology, or "NIST," has also taken great strides to collaborate with the private sector on developing a voluntary Framework of cybersecurity best practices. Last month, NIST published the latest version of its Framework to be even more informative and useful to a broader array of stakeholders.

In today's world, where information literally travels at the speed of light, and new innovations are brought to market at a dizzying pace, it is critically important to leverage robust information sharing about threats and vulnerabilities.

This should include greater information sharing about the supply chain of hardware and software that make up our communications networks.

When it comes to the supply chain, we must think about it over the long-term. We are fully aware of the issues that the President has raised regarding China, Huawei, and ZTE. We are also aware that the Department of Commerce has serious concerns. This point merits discussion, and it is the reason our hearing is so timely.

The quick and easy route would simply ban foreign vendors of vulnerable hardware and software from accessing our markets.

But the marketplace for hardware and software is global, and a hallmark of the communication industry is scale.

In time, it will be difficult for our domestic communications providers to obtain their network infrastructure from trusted sources when vulnerable foreign vendors acquire more and more global market share.

What are the implications of all this to our Nation's cybersecurity?

What are the implications for the race to 5G?

What are the broader implications to our economy?

And, most importantly, what are thoughtful solutions to such a complex problem?

These are some of the questions today's hearing seeks to address.

I am pleased to convene this hearing.

I look forward to the testimony of our witnesses.

And I yield 1 minute to the subcommittee's vice chairman, Mr. Lance.

Mrs. BLACKBURN. And at this time, I yield my remainder of time to Mr. Lance.

OPENING STATEMENT OF HON. LEONARD LANCE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. LANCE. Thank you, Madam Chairman.

This is a particularly timely hearing on an important topic. The security of our next generation networks is an issue that has come to the forefront. Earlier this year, a leaked memo from the White House recommended we nationalize our 5G network for national security reasons. While an extremely misguided and unrealistic approach, it is important that we secure our networks.

Just last month, the FCC voted unanimously to move a proposal forward to ban Federal funds from being used to purchase telecommunications equipment from companies deemed a security threat, such as Chinese manufacturers Huawei and ZTE. I commend Chairman Pai and the rest of the Commission for taking this important step.

ZTE has been deemed a security threat by our intelligence agencies and has been criticized by the Departments of Justice and Commerce for doing business in Iran and North Korea. Just yesterday, the nominee to head the National Counterintelligence and Security Center testified that Chinese intelligence uses Chinese firms such as ZTE as a resource, and he would never use a ZTE phone.

I am concerned about the national security implications of lessening the punishments against ZTE in a trade deal with China. National security and the security of our networks are primary concerns here, and the administration must consider that above all else in dealing with China.

I look forward to discussing this and other important issues surrounding the security of our telecommunications networks and the global supply chain with you today. Thank you.

[The prepared statement of Mr. Lance follows:]

PREPARED STATEMENT OF HON. LEONARD LANCE

Thank you, Chairman Blackburn and welcome to our distinguished panel.

This is a particularly timely hearing on a very important topic. The security of our next generation networks is an issue that has come to the forefront recently. Earlier this year a leaked memo from the White House recommended we nationalize our 5G networks for national security reasons. While an extremely misguided and unrealistic approach, it is important we secure out networks. Just last month the FCC voted unanimously move a proposal forward to ban Federal funds from being used to purchase telecommunications equipment from companies deemed a security threat, such as Chinese manufacturers Huawei (wah-way) and ZTE. I commend Chairman Pai and the rest of the Commission for taking this important step.

ZTE has been deemed as a security threat by our intelligence agencies and has been punished by the Departments of Treasury and Commerce for doing business in Iran and North Korea. Just yesterday, the nominee to head the National Counterintelligence and Security Center testified that Chinese Intelligence uses Chinese firms such as ZTE as a resource and he would never use a ZTE phone.

I am concerned about the national security implications of lessening the punishments against ZTE in a trade deal with China. National security and the security of our networks is the primary concern here and the administration must consider that above all else in their dealings with China.

I look forward to discussing this and other important issues surrounding the security of our telecommunications networks and the global supply chain with you today.

Mr. LANCE. Madame Chair, I yield back the balance of my time.

Mrs. BLACKBURN. The gentleman yields back.

At this time, Ms. Clarke, you are recognized for 5 minutes.

OPENING STATEMENT OF HON. YVETTE D. CLARKE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Ms. CLARKE. I thank you, Madam Chair, and I thank our witnesses for coming with their expert testimony this morning.

Communication networks in the United States increasingly rely on equipment and services manufactured and provided by foreign companies. According to the Government Accountability Office,

more than 100 foreign countries imported communications network equipment into the U.S. market between 2007 and 2011.

While the globalization of commerce and trade has created many benefits, these long supply chains have made it possible for bad actors to exploit vulnerabilities during design, production, delivery, and postinstallation servicing. The National Counterintelligence executive has noted that, quote, “The globalization of the economy has placed critical links in manufacturing supply chain under the direct control of U.S. adversaries,” end quote.

Some examples of the communications supply chain threats include attempts to disrupt the ability of an organization to operate on the internet; attempts to infiltrate a computer system to view, delete, and modify data; and attempts to use viruses or worms to extract data for use or sale. Some experts have even expressed concerns about the use of a kill switch, which could cause widespread communication outages and interruption in the power grid. And with the recent pronouncements of ZTE and Huawei, we know that this concern has been elevated to a national concern.

And so, today, we look forward to hearing from you your views and your insights into what we can do to make sure that the United States is well protected.

And I don’t know if I have any colleagues that are seeking any time.

Well, then, Madam Chair, I yield back.

Mrs. BLACKBURN. The gentlelady yields back at this time.

Mr. Walden, you are recognized.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you, Madam Chair, and thanks for holding this hearing on telecommunications, global competitiveness, and national security. These are really, really important topics this committee has dealt with before and will continue to deal with. As chairman of this very subcommittee back in 2013, I held a hearing on this same topic.

These are challenges that vex us, as demonstrated by our Subcommittee on Digital Commerce and Consumer Protection subcommittee’s hearing on CFIUS legislation last month.

Discussion on these topics usually happens in a classified setting, so there will be limits to the conversations we can have today, and we understand that. But as I mentioned, the Energy and Commerce Committee has the expertise on communications technology and a key oversight role in this debate.

For years, concerns have been raised about the supply chain and potential vulnerabilities that could be introduced into our communications networks. Of concern are foreign vendors that integrate seemingly private companies with their military and political institutions. There are also concerns about counterfeit equipment and fraud.

In more recent months, there have been alarm bells going off at all levels of Government about the potential threats to our communications networks. As startling as these threats are, some of the proposed solutions can, frankly, be even more distressing. Mr. Lance talked about that, I think, when that comment emerged

from the White House about nationalizing the system, I pointed out we are not Venezuela.

Before committees in Congress and different Federal agencies launch solutions to this complex challenge without proper coordination and investigation, I argue that we take a more thorough and thoughtful approach. Any net assessment of a serious challenge requires some fundamental questions be asked at the outset. These would include: How significant is this problem? Is it getting better or is it getting worse? What are the potential solutions and potential unintended consequences? And most importantly, in a resource constrained environment, how do you prioritize the solutions?

In the second half of the 20th century, we faced similar questions as our adversaries appeared to outpace us in strategic areas. In response, the United States invested heavily in research and development of cutting edge information and communications technologies. It is estimated the Government share of R&D at that time was two-thirds of the total U.S. R&D investment, and this laid the groundwork for both U.S. military superiority and unprecedented economic growth in America. But today, the ratio of Government to private R&D investments is completely reversed. Moreover, the barriers to entry in advance technology have been substantially reduced as costs have come down, research has globalized, and formally advanced technologies are now readily available.

So our competitors are more sophisticated than before, and some use their understanding of market dynamics to manipulate the market in their favor. And we simply can't replicate 20th century strategies for a 21st century economy. We have to be very wary of protectionist policies. As the chairman pointed out in her opening statement, the marketplace for technology is global. Nor can we rely on Government-centric approaches to simply spend our way out of this problem. Simply reacting to our competitors in symmetric tit-for-tat responses is never a winning strategy. If you are reacting, you are probably losing.

A better approach is to find and exploit the asymmetries that benefit us, the core competencies that define our economy and our society more broadly. This means development and early adoption of next generation disruptive technologies and doing that here. It means strengthening our private sector through greater information sharing about threats. It means better coordination among Government agencies so the private sector knows where to go when they encounter vulnerabilities in networks and not burdening them with redundant, conflicting regulations or unnecessary costs. It means greater dissemination of best practices and empowering the inclusiveness and transparency of standard setting bodies. We can either lead the world in these areas or we will have to follow it.

Today's hearing is a very important step in leadership. I appreciate the chairwoman's holding this hearing and her leadership on all of these issues, and I look forward to the testimony of our witnesses. I would tell you in advance we have two hearings going on simultaneously, no surprise for this full committee, so I will be coming and going, as will some other Members, but we do appreciate your contribution to our better understanding of the threats we face and the solutions that make sense in a global competitive environment.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Thank you, Madame Chairman. I want to welcome our witnesses to this hearing on “Telecommunications, Global Competitiveness, and National Security.”

These topics are not just timely, but ones which we have long set aside partisan differences, as we counter national security threats and empower our innovators to compete around the world. As chairman of this subcommittee in 2013, I held a hearing on this very same topic. These are challenges that still vex us, as demonstrated by our Subcommittee on Digital Commerce and Consumer Protection subcommittee’s hearing on CFIUS legislation just last month.

Discussion on these topics usually happens in a classified setting, so there will be limits on our conversation today. But, as I mentioned, the Energy and Commerce Committee has the expertise on communications technology and a key oversight role in this debate.

For years, concerns have been raised about the supply chain, and potential vulnerabilities that may be introduced in our networks. Of concern are foreign vendors that integrate seemingly private companies with their military and political institutions.

There are also concerns about counterfeit equipment and fraud.

In more recent months, there have been alarm bells going off at all levels of Government about the potential threats to our communication networks.

As startling as these threats are, some of the proposed solutions can be even more distressing.

Before committees in Congress, and different Federal agencies, launch solutions to this complex challenge without proper coordination and investigation, I argue that we take a more thorough approach.

Any net assessment of a serious challenge requires some fundamental questions be asked at the outset:

How significant is the problem?

Is it getting worse?

What are the potential solutions and potential unintended consequences?

Most importantly, in a resource constrained environment, how do you prioritize solutions?

In the second half of the twentieth century, we faced similar questions as our adversaries appeared to out-pace us in strategic areas.

In response, the United States invested heavily in the research and development of cutting-edge information and communications technology.

It’s estimated the Government’s share of R&D at that time was two-thirds of total U.S. R&D investment. This laid the ground work for both U.S. military superiority, and unprecedented economic growth.

But today, the ratio of Government-to-private R&D investment is completely reversed. Moreover, the barriers to entry in advanced technology have been substantially reduced as costs have come down, research is globalized, and formerly advanced technologies are now readily available.

Our competitors are more sophisticated than before, and some use their understanding of market dynamics to manipulate the market in their favor.

We cannot simply replicate 20th century strategies for the 21st century economy, and we must be wary of protectionist policies. As the chairman pointed out in her opening statement—the marketplace for technology is global.

Nor can we rely on Government-centric approaches to simply “spend” our way out of this problem.

Simply reacting to our competitors in symmetric, tit-for-tat responses is never a winning strategy.

If you are reacting, then you are losing.

A better approach is to find and exploit the asymmetries that benefit us—the core competencies that define our economy, and our society more broadly.

This means development and early adoption of the next generation of disruptive technologies.

It means strengthening our private sector through greater information sharing about threats.

It means better coordination among Government agencies, so the private sector knows where to go when they encounter vulnerabilities in networks, and not burdening them with redundant, conflicting regulations or unnecessary costs.

It means greater dissemination of best practices and empowering the inclusiveness and transparency of standards-setting bodies.

We can either lead the world in these areas, or we can follow it.

Today's hearing is a step in the direction of leadership, and I look forward to the captains of industry in technology and telecommunications heeding our call.

I thank the chairman for convening this hearing, and I look forward to the testimony of the witnesses.

Mr. WALDEN. Madame Chair, I yield back the balance of my time. With that, Madame Chair, unless any Members on the Republican side want the remainder of my time, I would be happy to yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Pallone, you are recognized for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Madame Chairman.

American broadband providers spend tens of billions of dollars every year to improve and extend our communications networks. The return on this investment is that our networks are fast, powerful, and global, but these benefits can be turned against us in an instant if the networks are not also secure. Every day, we hear about hackers cracking our systems and stealing our data, but another risk lurking in our networks may be even more dangerous: other nations quietly watching everything that we do online.

Unfortunately, a vast majority of our network equipment is now manufactured overseas by foreign companies. Most of this equipment works well and causes no problems, but our intelligence agencies have identified certain companies like Huawei and ZTE from China as posing specific threats to our national security. This equipment may have built in back doors that allow other countries to vacuum up all of our data. Once installed, these back doors can be nearly impossible to detect. And these risks are so serious that it led the Trump administration to float the idea of just building a federalized wireless network. While this solution was widely panned, the underlying threat that led to this proposal is real.

On the other hand, U.S. networks depend on equipment from foreign companies as they race to build next generation networks, like 5G wireless technologies. For many broadband providers, less expensive Chinese equipment may be the only option. And these issues are complex. But rather than crafting a coherent plan forward, the Trump administration has made this problem significantly more difficult.

With a tweet, the President muddled his own foreign policy, if he even had one, after the Commerce Department announced strong sanctions against ZTE for risking our national security. This weekend, the President tweeted that he is now worried these sanctions will cost jobs in China. And this makes absolutely no sense, in my opinion. That is why we need to hold more hearings like this one.

The public needs to hear more about the national security risks at play, and Congress needs to spend more time understanding potential options. The worst thing we can do is to rush to act without evaluating unintended consequences and whether certain proposals can even solve the problem.

But, unfortunately, some of our colleagues on the Armed Services Committee are suggesting we do just that. A proposal has been put forward as part of the National Defense Authorization Act that would cut off access to a wide array of network equipment without considering how to manage the risk to Americans. Worse, these provisions in the bill have been specifically crafted to circumvent our jurisdiction, and maneuvers like this rarely result in good policy.

Rather than take rash action, Congress must carefully craft a coherent plan subject to the rigors of regular order in the committees of expertise like ours. Our plan should make our networks both more robust and more secure. We are dealing with a complicated relationship between the future of our communications networks and national security, and these issues should not be taken lightly. So I urge my colleagues to oppose these efforts. We must find a proper balance that keeps our country safe, while ensuring that every American has access to powerful next generation broadband networks.

And finally today, Madam Chairman, I wanted to make a bitter-sweet announcement. Unfortunately, David Goldman, our chief counsel on this subcommittee, will be leaving at the end of this month to pursue an opportunity in the private sector, so this is actually his last hearing. He is over there on my left. And I say this is bittersweet because over the last 3 years, David has been an invaluable part of our committee team. He has provided us not only critical policy expertise, but also strong strategic guidance that helped lead to the passage of the bipartisan RAY BAUM's Act, for example, which included a lot of important Democratic priorities, including the SANDy Act.

And David, I think many of you know, has a long career of public service, including time at the FCC and in the Senate, God forbid, but, David, you will be missed, and we wish you nothing but the best in your future endeavors. Thank you so much. Thank you, David.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

American broadband providers spend tens of billions of dollars every year to improve and extend our communications networks. The return on this investment is that our networks are fast, powerful, and global. But these benefits can be turned against us in an instant if the networks are not also secure.

Every day we hear about hackers cracking our systems and stealing our data. But another risk lurking in our networks may be even more dangerous: other nations quietly watching everything we do online.

Unfortunately, a vast majority of our network equipment is now manufactured overseas by foreign companies. Most of this equipment works well and causes no problems. But our intelligence agencies have identified certain companies like Huawei and ZTE from China as posing specific threats to our national security.

This equipment may have built-in backdoors that allow other countries to vacuum up all of our data. Once installed, these backdoors can be nearly impossible to detect.

These risks are so serious that it led the Trump administration to float the idea of just building a federalized wireless network. While this solution was widely panned, the underlying threat that led to this proposal is real.

On the other hand, U.S. networks depend on equipment from foreign companies as they race to build next-generation networks, like 5G wireless technology. For many broadband providers, less expensive Chinese equipment may be the only option.

These issues are complex. But rather than crafting a coherent plan forward, the Trump administration has made this problem significantly more difficult. With a tweet, the President muddled his own foreign policy—if he had one. After the Commerce Department announced strong sanctions against ZTE for risking our national security, this weekend the President tweeted that he is now worried these sanctions will cost jobs in China. This makes absolutely no sense.

That's why we need to hold more hearings like this one. The public needs to hear more about the national security risks at play. And Congress needs to spend more time understanding potential options. The worst thing we can do is to rush to act without evaluating unintended consequences and whether certain proposals can even solve the problem.

Unfortunately, some of our colleagues on the Armed Services Committee are suggesting we do just that. A proposal has been put forward as part of the National Defense Authorization Act that would cut-off access to a wide array of network equipment without considering how to manage the risks to Americans. Worse, these provisions in the bill have been specifically crafted to circumvent our jurisdiction. Maneuvers like this rarely result in good policy.

Rather than take rash action, Congress must carefully craft a coherent plan subject to the rigors of regular order in the committees of expertise like ours. Our plan should make our networks both more robust and more secure. We are dealing with a complicated relationship between the future of our communications networks and national security. These issues should not be taken lightly.

I urge my colleagues to oppose these efforts. We must find a proper balance that keeps our country safe while still ensuring that every American has access to powerful next-generation broadband networks.

Finally today, a bittersweet announcement, David Goldman, our chief counsel on this subcommittee, will be leaving at the end of this month to pursue an opportunity in the private sector. This is his last hearing. I say this is bittersweet because, over the last 3 years, he's been an invaluable part of the committee team. David has provided us not only critical policy expertise but also strong strategic guidance that helped lead to the passage of the bipartisan RAY BAUM Act, which included a lot of important Democratic priorities, including the SANDy Act. David has a long career of public service—including time at the FCC and in the Senate.

David, you'll be missed, and we wish you nothing but the best in your future endeavors.

Thank you, I yield back.

Mr. PALLONE. I don't think anybody wants my time, so I will yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

And we add our well wishes to those that we are sending to David for a job well done and hope for the future.

At this time, this concludes our Member opening statements. All Members are reminded that, pursuant to committee rules, your statements will be made a part of the permanent record.

And to our witnesses, we welcome you. We appreciate that you are here today. As you see, this is something that has bipartisan concern and attention from our committee.

And for our panel for today's hearing: Dr. Charles Clancy, director and professor at the Hume Center for National Security and Technology at Virginia Tech; Ms. Samm Sacks, senior fellow at the Technology Policy Program at CSIS; and Mr. Clete Johnson, a partner at Wilkinson Barker Knauer.

You all are welcome. We appreciate that you are here today.

We are going to begin the testimony today with you, Dr. Clancy. You are now recognized for 5 minutes for your statement.

STATEMENT OF CHARLES CLANCY, PROFESSOR OF ELECTRICAL AND COMPUTER ENGINEERING AND DIRECTOR, HUME CENTER FOR NATIONAL SECURITY AND TECHNOLOGY, VIRGINIA TECH; SAMM SACKS, SENIOR FELLOW, TECHNOLOGY POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES; AND CLETE D. JOHNSON, PARTNER, WILKINSON BARKER KNAUER, LLP

STATEMENT OF CHARLES CLANCY

Dr. CLANCY. Thank you.

Chairman Blackburn, subcommittee members, my name is Charles Clancy. I am a professor of electrical and computer engineering at Virginia Tech. I am a recognized expert in wireless security, have held various leadership roles within international standards and technology organizations. And at Virginia Tech, I lead a major university program focused on the intersection of telecommunications, cybersecurity, and national security.

Prior to joining Virginia Tech in 2010, I served as a research leader in emerging mobile technologies at the National Security Agency.

It is my distinct pleasure to address this committee again on topics of critical national importance.

For the past 20 years, major forces have reshaped the telecommunications industry here in the United States and globally. Titans of the 20th century like Motorola and Lucent have faded and given rise to innovators of the 21st century like Apple and Cisco. These shifts have given birth to a global marketplace, which in turn has resulted in a global supply chain, a topic of interest in the hearing today.

Supply chains for telecommunications are complex, as has been noted. They include development of intellectual property, standards; fabrication of components and chips; assembly and test of devices; development of software and firmware; acquisition, installation, management of devices and operational networks; and the data and services that operate over those global networks. Competing in a global marketplace drives where and how each portion of the supply chain is executed.

An example I think that is pertinent is the modern supply chain of the Apple iPhone. Over 700 individual suppliers from 30 countries provide equipment and components into the Apple iPhone. It is one of the most sophisticated and complicated supply chains of any consumer electronic device, while the ultimate manufacturing happens in China where there are cameras from Japan, displays from Korea, and computer processors from Taiwan.

Only about 7 percent of the suppliers for the Apple iPhone are U.S.-based companies, to include chip manufacturers like Qualcomm and Intel, although their chips are actually manufactured in Korea and Taiwan. I think of note is the fact that much of the chip manufacturing industry is now offshore, with two-thirds of that industry operating out of China and Taiwan, and the United States only accounting for 8 percent.

Another interesting statistic to look at is standards. I personally have observed the rise of Chinese participation in standards bodies grow from almost nothing in 2005 to a commanding presence by

2010. By 2023, if current trajectories hold, Huawei will be the number one filer of intellectual property and the number one author of international standards within the Internet Engineering Task Force, outpacing Cisco in the next few years, based on current trends.

They have accomplished this not by buying American companies, but by buying American innovators with rigorous and competitive bonus packages for those who compete in these standards organizations. And this has happened completely—is invisible to the CFIUS process because it doesn't involve mergers and acquisitions.

So while several Chinese companies, as has been noted so far, have clearly taken shortcuts from theft of intellectual property to product sales to embargoed countries, China is undeniably part of the supply chain. So as mentioned, it is a complex ecosystem, and securing it requires, I think, a nuanced approach.

So as we look at securing the supply chain, I think the number one piece of advice is that really it needs to be an approach based on risk management. The supply chain threat—the cyber threat to the United States is real and tangible. Supply chain operations are among the most pernicious and difficult to detect. So a supply chain risk management approach that cuts across different technologies, sectors, and components of the supply chain I think is important.

One critical aspect of that is to look at the criticality of individual components. The criticality of a cell phone, for example, is very different than that of a core internet router. And so the risk management approach that goes along with that, I think, needs to reflect criticality of the component that is being considered.

I think that the NIST cybersecurity framework provides a great starting point for formulating such a strategy. It represents a shift away from a compliance-based approach, such as banning particular companies I think would be representative of a compliance-based approach to solving the problem, and more towards a risk management approach where the risks associated with the each component are quantified.

So recommendations moving forward. I think that we need a thorough assessment of supply chains for critical infrastructure. I think this needs to happen on a recurring basis. And where there are gaps, those gaps need to be identified and prioritized. Those priorities can then help inform how we foster a competitive domestic industry to fill those gaps in a way that those actions can be done in a globally competitive way.

Thank you.

[The prepared statement of Dr. Clancy follows:]

Testimony of Dr. Charles Clancy
Professor of Electrical and Computer Engineering, Virginia Tech
before the House Energy and Commerce Committee, Subcommittee on Communications and
Technology, Hearing on Telecommunications, Global Competitiveness, and National Security
May 16, 2018

Chairman Blackburn, Ranking Member Doyle, and Subcommittee Members:

My name is Charles Clancy and I am a professor of electrical and computer engineering at Virginia Tech, where I direct the Hume Center for National Security and Technology. In these roles, I lead major university programs in security, resilience, and autonomy. I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations including the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE). My current research sits at the intersection of 5G wireless, the Internet of Things, and cybersecurity.

I am co-author to over 200 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors.

Prior to joining Virginia Tech in 2010, I served as research leader for emerging mobile technologies the National Security Agency.

It is my distinct pleasure to address this committee again on topics of critical national importance.

Background

Over the past 20 years, major forces have reshaped the telecommunications industry in the United States and globally. As the industry has moved from delivering phone calls to delivering the Internet, American titans of the 20th century like Motorola and Lucent have faded and given rise to innovators of the 21st century like Apple and Cisco. These shifts have given birth to a global marketplace, which in turn has resulted in a global supply chain.

Supply chains for telecommunications are complex. They include development of intellectual property and standards; fabrication of components and chips; assembly and test of devices; development of software and firmware; acquisition, installation, and management of devices in operational networks;

and the data and services that operate over those networks. Competing in a global marketplace drives where and how each portion of this supply chain is executed.

An example of the modern supply chain is that of the Apple iPhone. Over 700 suppliers from 30 countries provide components. Component technologies come from all over the world and are assembled in China – cameras from Japan, displays from Korea, and computer processors from Taiwan. Only 7% of the suppliers are US companies, including wireless chips from Qualcomm and Intel, that are actually fabricated Korea and Taiwan. Note that generally with respect to chip fabrication, Taiwan leads with over 45% of global capacity, and China is number two at 20%. The United States only accounts for 8%.

Another interesting statistic to consider is contribution to the standards process. As someone who has participated heavily in international standards, I personally saw Chinese participation increase from zero in 2005 to a commanding presence by 2010. Huawei in particular leveraged a bounty system of bonuses to recruit away many of the most prolific contributors. In 2017, Huawei authored 21% of standards within the Internet Engineering Task Force, and was nearly tied with Cisco for the #1 filer of intellectual property claims. If the current trends hold, Huawei will be the world's top contributor to Internet Standards within five years, and the leading developer of associated intellectual property. Huawei accomplished this position not through buying American companies, but rather through buying American innovators, and therefore was invisible to the Committee on Foreign Investment in the United States (CFIUS).

While several Chinese companies have clearly taken shortcuts, from theft of intellectual property to revenue from product sales to embargoed countries, China is undeniably part of the global telecommunications marketplace and supply chain.

Securing the Supply Chain

Given this reality, questions of national security are critical. The cyber threat facing the United States is real and tangible, and supply chain operations are among the most pernicious and difficult to detect. The best approach for tackling this challenge is through thorough supply chain risk management.

In the telecommunications sector, there are varying degrees of criticality associated with core networking equipment, cell tower equipment, and individual smartphones. While recently there has been significant media emphasis on Huawei phones, Huawei also offers a complete line of core networking devices and cell tower equipment. In most every telecommunications subsector, Huawei's market share is in the top three, if not #1.

Consider the risks associated with latent malware on a core Internet router sharing bogus routing information with its peers – incidents in the past have demonstrated that accidental misconfigurations on a single router can take down significant segments of the Internet for extended periods of time. Imagine the impact if many routers acted in a coordinated fashion. This isn't about cell phones; it's about the survivability of the Internet itself.

As stated, it all comes down to risk management. Telecommunications companies need to consider the criticality of each component in their network, and the entire supply chain for each product they acquire and provision in their network. It is financially impossible to eliminate all risk, but supply chain risk needs to be assessed and quantified before it can be effectively managed. The overall trend in cybersecurity away from compliance-based security in favor of risk-based methodologies needs to be extended to supply chain, and the NIST Cybersecurity Framework is a great starting point for formulating such a strategy. Specifically, compliance-based approaches that ban specific vendors or products may offer near-term results but will not be durable approaches long term.

Recommendations

Looking forward, I encourage this subcommittee to consider the following.

First, supply chains for critical infrastructure are not well understood. There should be recurring assessments performed collaboratively between government and industry that examine each layer of the supply chain, from research and development through operations. Areas of risk should be identified and prioritized. Specific concerns about particular products or vendors should be shared with relevant industries. Those industries should, in turn, develop and implement risk management plans to address concerns.

Second, in areas where risk cannot be effectively managed unilaterally by industry, the US government should take actions to help foster the competitiveness of domestic industry to fill the gap. For example, these assessments can help inform the CFIUS process to promote more consistent and informed decisions regarding foreign acquisition of US companies. Other tools can be leveraged to help foster American innovation in gap areas to expand the pool of supply chain options.

Lastly, it is important that any actions taken to foster US industry in gap areas consider the global marketplace for telecommunications. Protectionist measures may help promote a domestic market, but in the long term companies will only be viable if they can compete internationally as the US is only around 20% of the global telecommunications market.

Thank you for the opportunity to address the subcommittee today and I look forward to questions.

Mrs. BLACKBURN. The gentleman yields back.
Ms. Sacks, you are recognized.

STATEMENT OF SAMM SACKS

Ms. SACKS. Madam Chairman Blackburn, Ranking Member Pallone, members of the committee, thank you for the opportunity to testify today.

My testimony reflects my experience as an analyst of Chinese technology policy for more than a decade. I have not only worked with the U.S. Government, but also in the commercial sector with leading multinational companies in China. These complex structural challenges require a deep understanding of the commercial and the national security dimensions of our trade and investment relationship with China.

The Chinese leadership is in the midst of building the most extensive Governance system for information communications technology of any in the world. This is part of President Xi Jinping's vision of building China into what he has referred to as a cyber superpower.

Today, I would like to discuss three implications for U.S. ICT companies doing business with China. First, companies face at least seven different kinds of security reviews of ICT products and services. These are essentially black box reviews. We have no idea what they will entail, in some cases, who will conduct them. They can cover network products and services, data that has to be exported, internet technologies. The list is broad, and it gives the Government discretion to do as it wants using these reviews as channels to review source code and also delay or block market access.

Second, many U.S. companies and China assume that data localization will be a reality of their operations in China, despite these rules still being in draft. Data localization is not only a market access barrier, but it is another tool for the Government to gain visibility into networks and digital information.

Third, U.S. companies face informal pressures in China, even in the absence of specific regulation. This is particularly in the case in areas referred to as core technologies where the Government has decided to double down on reducing reliance on foreign suppliers. This could include advanced semiconductors, certain kinds of software, the hardware and algorithms behind artificial intelligence systems.

So in short, the aperture for ICT companies doing business with China is rapidly closing. So what should be done?

We are correct to address areas where we have leverage with Beijing. We have seen that Beijing does not respond absent of external pressure. But the challenge is that U.S. Chinese and technology development, supply chains, commercial markets are tightly intertwined. Unilateral actions that isolate the United States will undermine U.S. economic prosperity, our technological leadership, and our capacity for innovation.

In confronting China, we must have a clear understanding about the consequences of our actions and where there will be costs to ourselves. I have three recommendations.

First, we should coordinate with allies and partners to create multilateral pressure. We have seen this work in the past. In 2009, a coalition of U.S., Japanese, European business and policy leaders created pressure that convinced China to suspend rules that would have required a type of surveillance screening software on computers in China. Unilateral action will compel China to retaliate against U.S. companies, leading Beijing to double down on the very structural problems that we are trying to address.

Second, we need channels to work with Chinese private sector players whose interests in some cases actually are more aligned with ours than some might think. Chinese companies need to compete globally in commercial markets and are often hindered by their own government.

Third, we must play offense by investing in our own R&D, infrastructure, STEM education, and a capital market that rewards investment. China will continue to invest in closing the technology gap with the United States regardless of U.S. actions, so we must be able to compete through our own technological and economic leadership.

Thank you. I look forward to your questions.
[The prepared statement of Ms. Sacks follows:]



**Statement Before the
House Energy and Commerce
Subcommittee on Communications and Technology**

***“Telecommunications, Global
Competitiveness, and National Security”***

A Testimony by:

Samm Sacks

Senior Fellow

Technology Policy Program

Center for Strategic and International Studies

May 16, 2018

2123 Rayburn House Office Building

Chairwoman Blackburn, Ranking Member Doyle, and Members of the Subcommittee, thank you for holding this hearing and for the opportunity to address these critical issues for U.S. economic and national security. My testimony today reflects my experience as an analyst of Chinese technology policy for more than a decade. I have not only worked with the U.S. government, but also in the commercial sector with leading multinational companies in China. The complex structural challenges posed by China's approach to technology and industrial policy require a deep understanding of both the commercial and strategic security dimensions of our trade and investment relationship.

The Challenge

The Chinese leadership is in the midst of building the most extensive governance system for cyberspace and information and communications technology (ICT) of any country in the world. A blend of national strategies, laws, regulations, and standards make up President Xi Jinping's vision of building China into a "cyber superpower" and "science and technology superpower."¹ Recognizing that technology has advanced more quickly than the government's ability to control it, Beijing has moved to rapidly to construct a policy and legal framework that will strengthen the Communist Party's hand not just over online content, but also the digital economy and the hardware and software that undergirds the internet.² President Xi has repeatedly stressed the need to bolster China's domestic ICT industry in order to reduce reliance on foreign core technologies.

The build-out of China's ICT governance system has implications for U.S. companies operating in China, as well as for Chinese investment flowing into the United States and globally. As this system takes shape, an accurate understanding of its elements and practical effects will be key for U.S. policymakers to calibrate the right response. There are substantial challenges from a national security and commercial perspective. Yet, U.S. and Chinese technology development, supply chains, and commercial

¹ <https://www.csis.org/analysis/cyber-policy-and-19th-party-congress>.

² <https://www.csis.org/programs/technology-policy-program/technology-and-innovation/cybersecurity-and-governance/china>.

markets are tightly intertwined in such a way that we risk undermining our own economic prosperity and our ability to maintain leadership in technology innovation without a targeted approach.

What Beijing Requires of ICT Companies in China

China's Cybersecurity Law (which took effect in June 2017) is the centerpiece of a much broader ICT regulatory system made up of dozens of interlocking parts. There are three main ICT regulatory concerns for U.S. companies operating in China: "black box" cybersecurity reviews, restrictions on cross-border data transfer, and an overall trend toward localization under the guise of security.

Cybersecurity Reviews

U.S. companies now face at least seven different ICT security reviews that can be used for political purposes to delay or block market access. These reviews will be conducted by different Chinese government agencies with unclear jurisdictions. There is even conflicting jurisdiction within individual reviews. Moreover, the specific criteria, metrics, and, in some cases, those conducting the evaluations are not known. As several U.S. industry representatives put it, the reviews are essentially a "black box" because we do not know what they entail and what is required to pass them. Some have lobbied the Chinese government to accept international security certifications (such as through ISO) as a basis for compliance, but so far it is not clear if Chinese authorities will recognize these certifications or still require their own reviews. Since there is no transparency into the process, these reviews can easily become political tools. The different cybersecurity reviews are discussed below:

1. The Multi-level Protection Scheme (MLPS): MLPS is managed by the Ministry of Public Security (MPS) and has existed since 2006. MLPS will likely undergo revisions as part of the new ICT legal regime, but coming changes, as well as how it will be coordinated with other similar security reviews, remain unknown. MLPS involves ranking networks by level of sensitivity, and then assigning certain compliance obligations.

2. **Cybersecurity Review Regime:** A key question is how MLPS will work in relation to a new review known as the Cybersecurity Review Regime (CRR) or Cybersecurity Review Measures of Network Products and Services. Issued in “interim” form in June 2017, the measures require network products and services used in critical information infrastructure (CII) to undergo a cybersecurity review administered by the Cyberspace Administration of China (CAC) and other sector-specific regulators. Some industry experts believe that the CRR will involve inspections of the backgrounds and supply chains of network and service providers. The final definition of CII is still pending, and the full criteria for assessments and list of those conducting them are unknown. Yet, without these pieces of the puzzle, the practical implications of this system remain murky.

The Chinese government has begun to issue several other documents meant to provide more clarity on the scope of the new review regime. These include the “Public Announcement on Issuing Network Key Equipment and Cybersecurity Special Product List (First Batch),” which outlines a list of products and services subject to the review and certification. There are also at least three relevant standards that have not yet been officially published. Yet, the follow-on product list and standards do little to narrow the far-reaching scope of the CRR. That is because the “interim” document establishing the CRR states that the review will focus on “other risks that could harm national security”—essentially preserving government authority to interpret the scope of reviews however it wants. Again, this is a channel that opens the door for political whim to determine market access.

3. **Reviews of Cross-border Data Transfer:** There will also be separate security review of data that companies seek to transfer outside of mainland China. The government is in the process of refining the process and conditions under which data would undergo a security assessment under two draft regulations: Personal Information and Important Data Cross Border Transfer Security

Evaluation Measures and Guidelines for Data Cross-Border Transfer Security Assessment. The specific scope is not yet clear, but according to industry sources inside China, it is likely that Chinese authorities will take a broad and ambiguous approach to enforcement of this particular review. (See following section on “Data Localization.”)

4. Cross-border Communications: Although not a security review per se, companies operating in China must have authorization from the Ministry of Industry and Information Technology (MIIT) for using internal company VPN (virtual private network) services. In practical terms, this means that the government reviews and approves the channels that companies use for all of their international connectivity. Requirements issued by MIIT in 2017 mandate that companies only use internal VPN services from licensed providers, which are the three state-owned telecommunications carriers. Cloud service platforms must route communications with their overseas facilities through channels approved by MIIT.
5. Internet Technologies and Apps: New technologies and apps used in internet news/information services also have a new security review process. Service providers must conduct security evaluations before the introduction of new technologies or applications on their platforms, but details are also murky.
6. A Possible Chinese Version of CFIUS: Much less is known about another possible kind of security review of foreign investment that has yet to emerge. China’s National Security Law (released in 2015) suggested in broad language there could be a new body perhaps akin to CFIUS. There has yet to been further clarification. New legislation expanding the scope of CFIUS could trigger Beijing to move forward setting up this new mechanism.

Data Localization

Many U.S. firms in China already assume that data localization requirements will become the de facto reality for their China operations. The specific scope of data localization requirements is still in flux; yet, some Chinese companies have even stopped sending their data to foreign companies that had the ability to store and process data within mainland China, despite there being no set requirement for them to do so. There are provisions still in draft form that would require certain kinds of data to be stored within mainland China and require approvals for cross-border data transfer. Below are the relevant laws, measures, and standards on the issue:³

According to article 37 of China's cybersecurity law: "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." The government is still defining "personal information and other important data" or what sectors fall under "critical information infrastructure" under separate measures and guidelines, but early indications suggest even follow-on directives will be vast and ambiguous. This also underscores the fact that China's ICT legal framework is best understood as a matrix of overlapping parts. Recently, Chinese officials have been asking U.S. government and business leaders for advice on how to define critical information infrastructure, suggesting the parameters are still in flux and open to interpretation.

Following on the Cybersecurity Law, the Chinese government issued a measure and standard meant to clarify the scope of how restrictions on cross-border data transfers will be implemented. The problem is that these follow-on directives are equally vague and leave issues unresolved as different stakeholders within the Chinese system debate their meaning. First is the "Measures on Security Assessment of Cross-border Transfer of Personal Information & Important Data (Draft for comment)." Companies have until December 2018 to comply. Several internal versions of the draft have been quietly circulated in the past few months. According to the latest publicly available draft, all "network operators" will be subject to

³ <https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect>.

assessments before exporting data out of China. In practice, this could mean anyone who owns and operates an IT network. Industry sources report the government may have walked this back recently to focus just on CII operators, but there is still tremendous regulatory uncertainty given that the definition of CII itself is up in the air. In addition, the National Information Security Standardization Committee (TC260)—China’s cybersecurity standards body—issued a standard to flesh out technical guidelines assessing cross-border data transfers.

Yet, the language even of this technical standard is extremely vague and far-reaching. The May 27, 2017 version gives a sweeping definition of “important data” that echoes the National Security Law, spanning that which can “influence or harm the government, state, military, economy, culture, society, technology, information . . . and other national security matters.” “Network operators” could mean anyone who owns and manages an IT network, raising the possibility that e-commerce could be deemed CII given all the personal data held by companies like Alibaba and Tencent. Depending on how CII is ultimately defined, many companies that are not in ICT sectors could potentially fall in scope. Chinese regulators are now studying how countries like the United States define CII through numerous Track 1.5 dialogues. While regulators are showing a willingness to engage and dialogue, it is not clear how these exchanges will ultimately impact Beijing’s policy trajectory, particularly since Beijing views this as primarily a national security rather than trade issue.

While China’s regulatory regime for data flows looks bleak, it is important to keep in mind that there are also competing voices in China advocating for more alignment with international practices. These voices should not be disregarded by U.S. policymakers. Key players in China think that cutting off cross-border data flows will hurt the country’s global economic goals. From national tech champions like Alibaba seeking global markets, to Chinese financial institutions facilitating global transactions, cross-border data flows are a core operational reality. These voices also exist within the Chinese government. For example, Hong Yanqing, who leads the personal data protection project for TC260, writes: “A fundamental consensus has emerged today that data naturally flows across national borders, that data flows produce

value, and that data flows can lead to flows of technology, capital, and talent.” These players could be important allies for the United States.

Localization Push under “Secure and Controllable”

U.S. companies face de facto localization pressures in China even in the absence of specific regulation. The Xi Jinping administration has emphasized through multiple channels that it seeks to bolster China’s domestic ICT industry to reduce reliance on foreign core technologies.⁴ A report by the National People’s Congress in December underscored the need for China to develop “indigenous and controllable core cybersecurity technology by 2020.” While there is official definition of what the government means by “core technologies,” authoritative documents indicate that the government is doubling down on indigenous development in fields such as advanced semiconductors, operating systems, cloud system, and the hardware and algorithms behind artificial intelligence systems.⁵

For several years, the government has used the phrase “secure and controllable” or “indigenous and controllable” in national strategies and directives as a way to link localization with security. Chinese companies have a competitive advantage when it comes to meeting these new security standards. This puts foreign ICT companies in a weaker negotiating position, and adds to pressure that they cooperate with local partners, rather than attempting to go it alone in the market.

The phrase has appeared in separate rules and strategies for cyberspace and the ICT industry. The phrase appears in sector-specific insurance, medical devices, and the Internet Plus sectors (i.e., smart technology, cloud computing, mobile technology, and e-commerce). A requirement for banking-sector IT to be “secure and controllable” was technically suspended, but many report that it still has negatively impacted market share. The phrase is also sprinkled throughout national-level blueprints for ICT

⁴ http://www.xinhuanet.com/2018-04/22/c_1122722221.htm.

⁵ <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/>.

development. For example, the 13th Five Year Plan for Informatization calls for “building a secure and controllable IT industry ecosystem.

Because this standard has no single definition, the government and Chinese industry have broad discretionary authority to launch intrusive security audits or reject foreign suppliers altogether as not secure. And while many of these regulations are still pending, Chinese government and industry are already moving forward with informal implementation of the standard, by asking foreign vendors to certify that they are “secure and controllable.”

Why the China Market Matters

Why do U.S. companies stay in such a high-risk and restrictive market? The answer is the size of the market—which accounted for \$23 billion of U.S. ICT exports in 2017—and its importance in the global supply chain. In addition, if major U.S. companies cannot operate and offer services in China, then they cede ground to Chinese companies since customers need to operate globally.⁶

China is not closed to all U.S. ICT firms or those with a digital footprint in the market. But the costs required to operate in China are increasing, particularly in high-tech sectors. Issues include ICT infrastructure—from trouble using corporate VPNs to the need to build local data centers—and lack of transparency around new licensing and security certifications that can be used to delay or block market access. Taken together, these new regulatory risks are now leading companies to reassess the tradeoffs required to make it in this important market.

Recommendations

There are substantial national security and commercial risks to the United States posed by China’s ICT policies and approach to developing its domestic industries. We are correct to address these issues and seek areas where we have substantial leverage with the Chinese government. After all, Beijing does not change its behavior absent external pressures.

⁶ <https://www.finance.senate.gov/imo/media/doc/11APR2018GARFIELDSTMNT.pdf>.

The challenge is that U.S. and Chinese technology development, supply chains, and commercial markets are tightly intertwined. A unilateral approach that isolates the United States will undermine U.S. economic prosperity, our technological leadership, and capacity for innovation. In confronting China, we must have a clear understanding about the consequences of our actions, and where there will be costs to ourselves. I have three recommendations:

First, we should coordinate with allies and partners to create international pressure on Beijing. Multilateral pressure has proven successful in the past. For example, in 2009 a coalition including the United States, Japan, and Europe combined efforts to pressure the Chinese government to suspend a requirement that screening software (“Green Dam Youth Escort”) with surveillance capabilities be installed on computers sold in China.⁷

Unilateral action will not only compel China to retaliate against U.S. companies, it will make Beijing double down on the very structural problems we want to address. Indeed, the Chinese government has drawn up retaliation lists of U.S. companies in China. U.S. companies with viable domestic competitors in China will be particularly vulnerable, and may see licenses canceled or denied under the umbrella of cybersecurity reviews and certifications, particularly of network products and services. This is not just a commercial issue, but also undermines security since many multinationals in China would be forced to rely on Chinese ICT companies for their business operations if US ICT companies left the market.

Second, we need channels to work with those Chinese private sector players whose interests are actually more aligned with ours than some may expect. There are examples in which Chinese industry has been an important ally to U.S. companies on pending regulatory issues. Companies like Alibaba looking to expand into global markets have an interest in allowing data to flow across borders. Since much of China’s ICT regulatory system is still in draft form, now is an important window to work with Chinese industry to push Beijing toward alignment with international best practices. The government cannot meet its goal of

⁷ <https://www.finance.senate.gov/imo/media/doc/11APR2018GARFIELDSTMNT.pdf>.

Sacks: Written Testimony, House Energy and Commerce Subcommittee 05/16/2018 11

having “big and strong Chinese internet companies” that can compete globally⁸ if these players are hindered by their own government. These local champions will become less helpful as trade tensions spill over to affect the broader bilateral relationship.

Third, we must play offense by investing in our own research and development (R&D), infrastructure, STEM education, and a capital market that rewards investment. China will continue to invest in closing the technology gap with the United States regardless of our actions, so we must be able to compete through our own technological and economic leadership.⁹

⁸ http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.

⁹ https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180126_Lewis_MeetingChinaChallenge_Web.pdf?ccS38O06FR8XG_vUn7GS1YrJXOTCZklM.

Mrs. BLACKBURN. The gentlelady yields back.
Mr. Johnson, you are recognized for 5 minutes.

STATEMENT OF CLETE D. JOHNSON

Mr. JOHNSON. Thank you for the opportunity to share my perspective with you on this critical, bipartisan issue. My testimony today reflects lessons from my experience with supply chain security issues, multiple Government-private sector positions, including as a logistics officer in the U.S. Army and as counsel for the Senate Intelligence Committee, the FCC, and the Department of Commerce.

Now at Wilkinson Barker and Knauer, I advise clients navigating this complex security and market environment, particularly through partnership with the Federal Government. My advice to clients also draws on these experiences, but the views I express today are my own.

This committee well knows that the global supply chains for hardware-software services that make up the world's internet and communications technology ecosystem raise complex national security, strategic, economic, business, and technological concerns. The United States has long played the leading role in advancing these world changing tech developments, and addressing security concerns in a way that further advances these innovations is absolutely crucial to maintaining that U.S. leadership.

As we advance to a thoroughly connected 5G world, the capability of bad actors to use these technologies and to leverage their supply chains for IP theft, cyber espionage, sabotage, and even warfare presents acute threats. These are well-funded, purposeful, sophisticated nation-state adversaries, spies, criminals, other malicious actors, and they are working hard to find openings for their nefarious purposes. And many such openings are there to be found.

The threats and vulnerabilities are real and they manifest in different ways at all levels of the global supply chain, beginning with the Chinese and Russian companies identified in recent Government actions. The actions that Congress and the administration have taken in recent months to address these concerns constitute a significant and welcome intensification of policy activity. We are at an inflection point on these issues for good reason, and we need to do this right. The issues are highly complex, as has been noted, and solutions must take root in a global market in which rapid business developments and the practical realities of the supply chain challenge traditional boundaries and legal jurisdictions. The challenges call for private sector leadership in close collaborative engagement with Government partners through clear and effective processes.

In recent months, there have been more than a dozen new Government actions on these issues, and perhaps the most important is the FCC proposal championed by Chairman Pai and unanimously adopted last month to prevent Government funds from purchasing technology or services from companies that pose a national security threat to U.S. communications infrastructure.

This process will significantly advance this policy discourse and can be a lever to move the whole Government and the market in the right direction. The market needs clear, practical guidance that

derives from well-informed processes with input from experts from throughout the Government as well as from the private sector stakeholders who know the market best.

Restrictions on the three companies identified in last year's defense authorization act are really the easy step. The more difficult questions have to do with how these policies will be implemented, how they will be updated, possibly expanded in the future.

So a few high level thoughts on the FCC proposal, which is targeted to address supply chain security for networks supported by public funds but has implications that are precedent setting and potentially much more far reaching.

Identifying national security threats is a function of our intelligence, law enforcement, defense, and homeland security agencies, so as the FCC implements this rule, there will need to be thorough coordination through the Government to ensure that new requirements are fully aligned with national security decisions by the administration and Congress and that they derive from broader inter-agency policy processes or statutory requirements.

DHS, as the sector-specific agency for the communications and IT sectors should coordinate these efforts with lots of input from the Department of Commerce as well as input from the Departments of State, Justice, Defense and, yes, the FCC. To promote a collaborative partnership with industry, sensitive private sector information should be formally protected under the Protected Critical Infrastructure Information Act, which prohibits disclosure of protected information under FOIA and use in litigation or regulatory enforcement actions.

In short, the FCC's actions in the month and years ahead should derive from and they should further advance processes that are built on principles of industry leadership and Government-industry partnership.

I look forward to further fleshing out these thoughts in answers to your questions. Thank you.

[The prepared statement of Mr. Johnson follows:]

**Summary of Statement of Clete D. Johnson
Partner, Wilkinson Barker Knauer, LLP**

**Committee on Energy and Commerce, Subcommittee on Communications and Technology
U.S. House of Representatives**

**Hearing on Telecommunications, Global Competitiveness, and National Security
May 16, 2018**

Supply chain security issues are crucial for American technology leadership and the future of our economic and national security. My testimony today reflects lessons from my experience with these issues in multiple government and private sector positions, including as counsel for the Senate Select Committee on Intelligence, the FCC, the Dept. of Commerce, and private practice.

The supply chains for the global internet and communications technology ecosystem raise complex national security, strategic, economic, business, and technological concerns. The United States has played the leading role in advancing these tech developments, and we must address these security concerns in a way that further advances innovations and U.S. leadership.

The capability of bad actors to use these technologies – and to leverage supply chains – for intellectual property theft, cyber espionage, sabotage, and even warfare presents acute threats. There are well-funded, purposeful, sophisticated adversaries, spies, criminals and others who are working hard to find openings for their nefarious purposes. These threats and vulnerabilities manifest in different ways at all levels of the global supply chain, beginning with the Chinese and Russian companies that have been identified in recent government actions.

The public actions that Congress and the Administration have taken in recent months to address these concerns constitute a significant, and welcome, intensification of policy activity.

We need to do this right. These issues are highly complex, and solutions must take root in the global market. These challenges call for private sector leadership, in close, collaborative engagement with government partners through clear and effective processes.

Perhaps the most important of recent actions is the FCC proposal to prevent government funds from purchasing technology or services from companies that pose a national security threat to the U.S. communications infrastructure. This will advance the policy discourse on these difficult issues and can be a lever to move the whole government, and the market, in the right direction.

The market needs clear practical guidance that derives from coherent, well-informed processes that include input from experts throughout the government, as well as from the private stakeholders who know this complex market best. This should be led by DHS, and the confidentiality of sensitive private sector information should be protected.

The FCC's actions in the future should derive from, and further advance, processes that are built on principles of industry leadership and government-industry partnership in cybersecurity and supply-chain risk management.

**Statement of Clete D. Johnson
Partner, Wilkinson Barker Knauer, LLP**

**Committee on Energy and Commerce
Subcommittee on Communications and Technology
U.S. House of Representatives**

Hearing on Telecommunications, Global Competitiveness, and National Security

May 16, 2018

Chairman Blackburn, Ranking Member Doyle, distinguished Members of the Subcommittee, thank you for holding this hearing. These issues are crucial for American technology leadership and the future of both our economic and national security, and I thank you for the opportunity to share my perspective on this critical bipartisan policy activity.

My testimony today reflects insights and lessons from my experience with supply chain security issues in multiple government and private sector positions since I was a logistics officer in the U.S. Army in the late 1990s. Over the past dozen years, these experiences have focused on promoting private sector leadership in cybersecurity and national security-based export controls in the global market for internet and communications technology, including through crafting legislation and conducting congressional oversight as counsel for the Senate Select Committee on Intelligence and working through regulatory proceedings and interagency National Security Council processes as counsel at the Federal Communications Commission and the Department of Commerce.

Now at Wilkinson Barker Knauer, I advise a number of clients on how to navigate this dynamic, complex and fast-changing global market and security environment – particularly through partnership with the federal government in advancing our collective security. I would

like to note that while the advice I provide clients also draws from these same experiences, the views I am expressing today are my own.

As this Committee well knows, the global supply chains for the diverse and innovative hardware, software and services that make up the world's internet and communications technology ecosystem raise a complex mix of national security, strategic, economic, business, and technological concerns. The United States and its innovative companies and people have played the leading roles in creating and advancing these world-changing tech developments, and addressing security concerns in a way that further advances these innovations is absolutely crucial to maintaining that U.S. leadership role and our society's prosperity. As we advance to a thoroughly connected 5G world, the capability of bad actors to use these technologies – and to leverage their supply chains – for intellectual property theft, cyber espionage, sabotage, and even warfare presents acute threats. There are well funded, purposeful, sophisticated nation state adversaries, spies, criminals and other malicious actors who are working hard to find openings for their nefarious purposes – and many such openings are there to be found.

These threats and vulnerabilities are very real, and they manifest in different ways at all levels of the global supply chain, ranging from the Chinese and Russian companies that have been identified in recent government actions all the way down to small startups in Silicon Valley or elsewhere that few have even heard of.

The public actions that Congress and the Administration have taken in recent months to address these concerns constitute a significant, and welcome, intensification of policy activity that has been percolating for a decade. We are at a policy inflection point on these issues, for good reason, and we need to do this right. These issues are highly complex, and solutions must take root in multiple arenas of a global market in which rapid business developments and the

practical realities of the supply chain can challenge or blur traditional boundaries and legal jurisdictions. These challenges call for private sector leadership – in close, collaborative engagement with government partners through clear and effective processes.

In recent months, more than a dozen new government actions on these issues have either taken place or are presently pending. Perhaps the most important of these activities is the FCC Notice of Proposed Rulemaking, championed by Chairman Pai and unanimously adopted last month. This proposal, which would prevent government funds from purchasing technology or services from companies that pose a national security threat to the U.S. communications infrastructure, will significantly advance the policy discourse on this difficult set of issues. Moreover, I believe this proposal can serve as a lever to move the whole government, and the market, in the right direction. Put simply, the market needs clear practical guidance that derives from coherent, well-informed processes that include input from experts throughout the government, as well as from the private stakeholders who know this complex market best.

Prohibitions or restrictions on the Chinese and Russian companies identified in last year's National Defense Authorization Act and cited in the FCC's Notice are perhaps the easy step. The more difficult questions over the longer term have to do with how these policies will be implemented and updated – or possibly expanded – in the months and years to come.

With this in mind, I would like to offer a few high-level thoughts on the FCC proposal. While the FCC has targeted its action to address supply chain security issues pertaining to networks supported by public funds, the implications of the FCC's precedent-setting proposal are potentially far-reaching. The identification of national security threats is fundamentally a function of the intelligence, law enforcement, defense and homeland security agencies of the Executive Branch, so as the FCC implements this rule, there is a need for thorough coordination

throughout the federal government in order to ensure that the supply chain security requirements or prohibitions for recipients of public funds are fully aligned with national security policy decisions by the Administration and/or Congress. Over the long term, the FCC should ensure that any further requirements or prohibitions derive directly from broader interagency policy processes or statutory requirements.

The Department of Homeland Security, as the Sector Specific Agency for the communications and information technology sectors, should coordinate these efforts, with input from the Departments of Commerce, State, Justice, Defense and others. The recently-begun Telecommunications Supply Chain Risk Assessments by DHS's Office of Cyber and Infrastructure Analysis could provide the basic foundation of such a process. To promote candor and collaborative partnership with industry leaders, sensitive private sector information provided by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits disclosure of protected information under the Freedom of Information Act or state transparency laws, and use in civil litigation or regulatory rulemaking or enforcement actions.

In short, the FCC's actions in the months and years ahead should derive from, and further advance, processes that are built on principles of industry leadership and government-industry partnership in cybersecurity and supply-chain risk management. I look forward to further fleshing out these thoughts in answers to your questions.

Mrs. BLACKBURN. The gentleman yields back.

And we thank you all for your statements. I will begin the questioning and recognize myself for 5 minutes.

Mr. JOHNSON, I want to come to you first. You talked about in your testimony how complex this challenge is and the need for collaboration, and I think we all agree with that. And we appreciate your background and the holistic view that you bring to looking at this and you know how and are familiar with the legislation passed in 2015 and how that looks at a clear and effective process for the public-private collaboration in the cyber realm. But the law was not designed for threats to the supply chain. And Ms. Sacks mentioned data transfer and things of that nature in her testimony.

So let's look at and talk about a formalized process for information sharing for the supply chain between the public and the private sectors, and I would like to hear you weigh in on that.

Mr. JOHNSON. Absolutely. And, Madam Chairman, you and your colleagues on both sides of the aisle and both sides of this Hill should be commended for the landmark legislation, the Cyber Information Sharing Act. What it provided were paths and legal clarity on the types of cyber threat information that can be shared between industry and the Government, and Government back to industry, and also between industry players, along with privacy protections and other protections.

And what that—that was a landmark effort because it created protections for that sharing that provide general counsels and companies across the country certainty that if they are engaging in this type of sharing, they are not—they are actually helping their legal risk posture as opposed to contributing to it or taking risk.

What it did is it focuses on tactical and operational information sharing. It is basically sharing ones and zeros digitally and by machines. So it is about the here and now threat environment and what is happening on the network in this instance. And it is about diagnostic type information.

What we need in this supply chain arena, and I mentioned the protected critical—excuse me, Protected Critical Infrastructure Information Act, and we will talk about that a little bit more, what we need is more of an operational and strategic. So as opposed to tactical and operational, you start with operational, but it is also a strategic engagement between private sector entities and the expert Government agencies about candid assessments of what they are doing, what is working, what is not working, and in the area of supply chain, what they have, what they are seeing, what they are worried about, and what the Government is worried about.

Mrs. BLACKBURN. OK. Let me ask you about that. We have done a lot of work in this committee on rural broadband, and Ms. Clarke and I have done a lot of work together on unserved areas. Whether it is urban, as in her district, or rural, as in my district. So when you look at that, how do you ensure that supply chain information sharing is disseminated to those smaller broadband providers, whether they be urban, as in her district, or rural, as in mine? Because they really do lack the staff and the sophistication to handle that.

Mr. JOHNSON. That is a great way to look at that question because it speaks to what is the value to the company of this engage-

ment. Are they doing it as a service to the Government? Are they taking extra time to do it? Or is it something that adds value to their bottom line because it creates efficiencies and an information environment that they need but they don't have other ways to get?

So the best way to provide value to those low-margin rural and urban smaller providers is to make it worth their while to come in and talk to the Government about what they see, what they have got, and how the Government can help them, including by giving them clear guidance about it is not a good idea to go in this direction.

Mrs. BLACKBURN. I thank you for that.

I have only got 30 seconds left. And, Ms. Sacks, I have got, let's see, three questions that I wanted to come to you on, but I tell you what I am going to do. I am going to submit them for the record for you to answer back to us. Because I appreciate your testimony and how you laid out what you think the challenges are and then laid out the three steps, and I wanted to drill down on that a little bit further, but I will submit this.

I yield to Ms. Clarke 5 minutes for her questions.

Ms. CLARKE. I thank you, Madam Chairwoman.

As American companies continue to work through preparations for 5G, we often focus on domestic issues. And I think that taking such a narrow approach can cause people to overlook the issues with making foreign components so integral to our supply chain. For instance, small businesses can often only get access to foreign-made equipment, which is often less expensive. But this equipment is also more likely to be subject to sanctions. For all the steps the FCC is taking to eliminate deployment regulations, it won't matter if providers can't get access to equipment made by other manufacturers.

So, Mr. Johnson, just drilling down on the practical applications, what does the landscape look like for small businesses who use Huawei and ZTE equipment?

Mr. JOHNSON. It depends company by company. I think looking across the country, there are a number of providers of the various types of equipment and services that Huawei and ZTE provide, and I think that will be the case regardless of their status in the U.S. market. They have a relatively small share of the U.S. market. I think in Huawei's case, I think their U.S. revenue is less than 1 percent of their global revenue. And in each of the areas that they lead various types of equipment, various types of devices, various types of services, there are robust competitors in each of those arenas, as well as, you know, both in the case of global companies and also in the case of smaller startups that are trying to break into the market.

So the record that is being created at the FCC, this is one of the reasons why this is such an important proceeding. For the first time, on June 1, with all the comments due on that proceeding, there will be a public record to answer this question, what is the effect, and then there will be another reply round. And I think we are going to get a lot of information out of that that will help illuminate how this affects individual companies and how it affects certain parts of the market.

Ms. CLARKE. So do you think that the domestic manufacturing market is capable of filling those gaps left by Huawei and ZTE?

Mr. JOHNSON. I think that the—as Dr. Clancy mentioned, the market has changed in pretty significant ways in recent years, and it might be better to say it as opposed to domestic manufacturing, there certainly is domestic manufacturing in some areas, but it may be better to look at it as a trusted supplier manufacturing, which can take—can span continents and often does touch China. And the competition among trusted suppliers is robust and dynamic, and I think that if there is a small vacuum that is created by any prohibition or restriction pertaining to Huawei or ZTE, that market will probably respond to that pretty quickly.

Ms. CLARKE. So to the panel, given that many small businesses serving low-income communities rely heavily on ZTE handsets, I am particularly concerned about the fallout of the sanctions on Lifeline subscribers. What role can Congress play in easing some of the burdens small businesses will encounter in replacing ZTE handsets with secure alternatives? Any ideas out there?

Dr. CLANCY. I would say that we need to differentiate a handset from a core internet router. There are very different risks associated with that. The risks associated with a ZTE handset, in my opinion, are much lower to national security than, for example, having core internet routers or core cellular network or 5G equipment from ZTE. So I think, in particular, as you look at the NDAA language, the ability to clarify the difference between core infrastructure and edge devices is important and would help, I think, address your concern.

Ms. SACKS. I would like to add to Dr. Clancy's comments that we leave it to the security experts to differentiate among the specific risks and design mitigation strategies around that, particularly as Chairman Walden mentioned, we need to prioritize resources accordingly. I think it is important that the United States does not take a sweeping approach to banning companies based on national origin, but instead, looks at the specific threats posed by equipment. And policies need to also take into account the fallout, the repercussions for U.S. companies and the U.S. economy to those approaches.

Mr. JOHNSON. Ma'am, I would add to that that the threat based on handsets and individual devices is narrower. It does pertain potentially to the holder of that device, but probably only to that person. And so there is an issue of if you are a sensitive person, you probably want to be careful about what device you hold. And I think as we move forward through this process, we want to make sure that low-income people are not are not the subject of lesser security than sensitive personnel are.

Ms. CLARKE. I yield back, Madam Chair. Thank you very much.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Latta, 5 minutes.

Mr. LATTA. Well, thank you, Madam Chair. Thanks very much for having this hearing today. It is very, very important.

I want to thank our panelists for being with us today, because we have talked about this issue in many hearings and a lot of outside discussions as to how critical this is.

And if I—Dr. Clancy, if I can start with you. In your testimony, you talk about the risk management that comes down to telecommunications companies need to consider. You say the criticality of each component in their network and the entire supply chain for each product, and you also say it is financially impossible to eliminate that risk. And at the same time, in your testimony, you talk about the over 700 suppliers from 30 countries that provide components, and you are talking about the Apple iPhone, with only 7 percent of that coming from U.S. companies.

How do we give confidence to the consumers out there through the companies that, you know, these products that they are using are secure, when we see from your testimony at the same time that, you know, it is impossible to eliminate all that risk at that time?

Dr. CLANCY. So my comments with respect to the iPhone were merely to illustrate how complex supply chains are and how many different parts of the world they touch, not necessarily indicating that that particular supply chain posture is good or bad. I think that from a consumer perspective, there needs to be confidence that the products and services that they are using meet their security thresholds. I think you also need to consider the motivations of hackers and adversaries.

The specific comment about being financially and feasible to eliminate all risk, any determined adversary with enough time and resources is going to be able to penetrate a target network. So as you look at a risk management approach, you need to be able to identify what the most sensitive parts of your network are, be able to fortify those as much as possible against those risks, whether it be a supply chain risk or it be an active cyber attack risk, and then make sure you are prioritizing those investments based on the criticality of the individual components.

So I think that would be—again, my view, again, supply chain risk management looking at criticality of the devices, how the devices are used in the network, and the supply chains associated with each one I think is really, I think, the best strategy.

Mr. LATTA. Let me follow up with another question to you. As the FCC, Congress, and other Federal agencies look at ways to prevent public funds from supporting suppliers that pose a threat to national security, who should be making the determinations as to which suppliers pose a real threat?

Dr. CLANCY. So that is an excellent question. Obviously, we have seen either regulatory or legislative approaches to selecting those companies. I think that that process is, I think, perishable, and there needs to be a more modular way of identifying risks in the supply chain. While companies like Huawei, ZTE, and Kaspersky as well may represent specific examples of supply chain risk, there are many component vendors as well that may present supply chain risk, depending on the type of equipment they are being integrated into.

So I think there needs to be a role within the Federal Government for assessing and understanding the entire supply chain and assessing the risk of specific vendors in that supply chain. And then, as the chairwoman and Mr. Chairman mentioned, was the ability for that information to be shared with industry as they look

to construct and manage the risk associated with their supply chain.

Mr. LATTA. One more question, and I am not picking on you here. Is there sufficient competition in the vendor markets to even allow a telecommunications provider to have realistic options to purchase economical and secure equipment?

Dr. CLANCY. I believe so. I think that, as was pointed out, the Huawei market share and ZTE market share, for example, is very small, and there are a number of other vendors of similar price point equipment that could be selected as an alternative. I think that we may need investment in U.S. industry, identify where the gaps are in U.S. supply chain in particularly critically important aspects in order to foster domestic competitiveness on a global market in order to expand options.

Mr. LATTA. Let me ask, how do we foster that to get that more competitiveness than in the U.S. market?

Dr. CLANCY. So depending on precisely where the risk is, you could look at research and development investments, you could look at economic investments to try and bolster particular industries. Let's say, for example, there was an effort to—there was a determination that the fact that we have all of the chip manufacturing is happening offshore, right, I think that could be an area where if you want to foster a chip fabrication industry in the United States, there are a wide range of incentives that you can put together to try and accomplish that. Now, whether or not that makes economic sense, I don't know, but I think there are levers there.

Mr. LATTA. Thank you. Madam Chair, my time has expired, and I yield back.

Mrs. BLACKBURN. Mr. Pallone, you are recognized for 5 minutes.

Mr. PALLONE. Thank you, Madam Chairman.

The threats to our network supply chain pose a serious national security risk, and I don't think forcing through provisions as part of the National Defense Authorization Act is the best process. So I ask Chairman Walden and Chairman Blackburn and the rest of my colleagues on our committee to work together to pursue thoughtful legislation. Because these security risks pose an urgent threat, I hope we can work together to quickly pass a bipartisan proposal. My questions will therefore focus on how to craft the right policies for our country.

Mr. JOHNSON, in your written testimony, you suggest using the interagency process to reach a better informed result, and some may believe that an interagency process is too slow, however, to deal with the immediacy of this threat. So let me start with Mr. JOHNSON. If Congress were to pass legislation setting out an interagency process to address supply chain risks, what is the fastest you think the executive branch could act to protect our supply chain? Is 180 days possible, for example?

Mr. JOHNSON. Congressman, I think the executive branch is already taking steps in that direction, and also already has models for interagency collaboration, particularly through a partnership of the Department of Homeland Security and Commerce leading this botnet reduction initiative under the executive order, for instance. So I think the muscle memory is there, and with apologies to former overworked colleagues in the executive branch, I think some

pretty big steps could be taken in 180 days. And the only thing I would add is that it would need to continue on day 181 and beyond. So this process will never be finished. Kind of like the NIST framework, it will always be being improved.

Mr. PALLONE. Well, thank you. I said that I was concerned that the proposals being considered as part of the National Defense Authorization Act are static and would not evolve with the changing threats to our supply chain. A solution that only addresses the risks we face today I think could simply give foreign actors a blueprint for avoiding our protections for tomorrow.

So again, Mr. Johnson, if we are actually going to create lasting protections for our supply chain, how should we craft laws so they can respond to new and emerging threats?

Mr. JOHNSON. I think the answer to that is that continuous process, and it should include those two departments that I have mentioned. It should include the FCC, as well as possibly other regulatory agencies, as well as State, Justice, FBI, Defense, potentially other agencies. And crucially it should include the opportunity for private sector entities who know the market best and know the corners that the Government doesn't necessarily see. It should provide opportunities for them to come in in a candid, collaborative way, say here's what we are seeing, here's what I am picking up, and here's what my concerns are, and here's what the market bears. All of that is relevant to this.

And as Dr. Clancy and Ms. Sacks noted, distinguishing between different components and parts of this market is crucial and complex, and you really can't do that without this holistic look of all the elements of Government and relevant players in the private sector.

Mr. PALLONE. All right. Thanks. And my last question, which I can get—any of you could answer, is I believe, as I said, the committee should work together to produce informed and well-reasoned bipartisan legislation to secure our supply chain. So with that in mind, could each of you tell me what you believe is the one thing we should include in a bill to protect our critical networks? And we have only got a minute and a half, but let me start with Dr. Clancy and we will go down.

Dr. CLANCY. I think this—just generally, this notion of not—any focus on specific companies will have perishable impact, so there needs to be a modular approach to identifying what particular components of the supply chain are of the most risk.

Mr. PALLONE. Ms. Sacks. Thank you.

Ms. SACKS. We need to be careful not to replicate the China model in terms of picking winners and losers and using a state-led approach that doesn't enable the industry and investment to do as it should. So we have an opportunity for technological leadership by enabling R&D, enabling more STEM education in a way that shows a U.S. versus a state capitalist model in technological development.

Mr. PALLONE. Thank you. Thirty seconds. Mr. Johnson, 30 seconds left.

Mr. JOHNSON. I agree that the private sector perspective is crucial to not be eclipsed by the Government perspective. And so I think clarity in the process in making clear what the—who is in

the lead, who is putting in what inputs from the interagency so that private sector companies can navigate that is crucial, as well as legal mechanisms that allow them to feel protected in candid collaboration with the Government.

Mr. PALLONE. Thank you. I yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

Mr. JOHNSON. You are recognized.

Mr. JOHNSON OF OHIO. Thank you, Madam Chair.

I would like to—Mr. Pallone, most Johnsons can't even say their name within 30 seconds. He did a really good job of staying in that timeframe there. So thank you.

Dr. Clancy, you know, some of the more concerning threats arise from the ongoing access that vendors have. What is the scope of this access? Are the threats limited to software or firmware updates, or could the ability of a technician to replace and repair parts also introduce risks?

Dr. CLANCY. So as you look at many of these vendors' networks, Huawei would be a good example, they have deployed telecommunications infrastructure globally, core switches and routers throughout many countries all over the globe. And as was mentioned, that market share here in the U.S. is fairly small. Part of that involves a service agreement where the operator has reach back in order to get service and support that they need as part of that purchase of equipment. So whether it is these devices doing software updates and getting new firmware loaded or its vendors who are working under a support contract are able to log in and access those systems, both of those represent operational security risks associated with use of that equipment in the environment.

Mr. JOHNSON OF OHIO. Well, using a risk management approach, how would a smaller rural provider that relies on these kinds of services manage these kinds of threats?

Dr. CLANCY. That is a great question. I think that the—I think the NDAA language suggests that in certain situations if the equipment is used, that any remote access be blocked. That also has challenges because if you are now blocking software updates, you may be blocking the ability to address vulnerabilities in the product that anyone could take advantage of, not just the vendor.

So I think, again, if you are looking at what equipment should be deployed in a small rural internet service provider, I think that I would steer away from those that would have risks, such as the companies that have been identified. But that list should not be static, and there needs to be a way to continually provide industry with best practices about what products to use, which products potentially to avoid, and the risks associated with that.

Mr. JOHNSON OF OHIO. I guess it raises another question what the alternatives might be. I am a software engineer by trade. I spent 30-plus years developing and implementing software both within the Government and without. And, I mean, the way we used to do it, there used to be a third-party organization, a black hat organization if you will, that tested everything and had the security and access and the security privileges to be able to do that. The providers themselves, the vendors themselves weren't allowed to put their hands on the operational system. What alternatives do you see for the situation?

Dr. CLANCY. So I think there has been a fundamental shift in the market in the last probably decade towards managed services. With the growth of the cloud and everything as a service, people want telecom equipment as a service, and who better to provide that service than the vendor of that equipment.

I think it might be very interesting for a managed service ecosystem to grow here in the United States that could be a third party to provision and manage those devices on behalf of some of the smaller operators. I don't know the extent to which that industry is mature right now because the vendors, for the most part, are providing that as a benefit of buying their products.

Mr. JOHNSON OF OHIO. Well, thank you.

Mr. Johnson, DHS recently announced that they are kicking off two investigations into the security of our Nation's telecommunications supply chain, both from a general perspective and with regard to specific vulnerabilities. Can you think of anything else that DHS, FCC, or other Federal agencies can examine to better address the holistic set of threats that our telecommunications infrastructure faces?

Mr. JOHNSON. Yes, sir. And I think that that initiative—

Mr. JOHNSON OF OHIO. You have got 30 seconds.

Mr. JOHNSON. I will do it quickly again. I am from Georgia, but I will try to talk fast.

That particular initiative that has just kicked off I think can be the beginning and the foundation of the broader interagency and public-private look at these issues and inquiry that we need to have. The FCC process that is going on will conclude a comment period on July 2, will add a lot of value to that, and there is some other processes going along, and I think the importance is to integrate all of that learning into a navigable set of processes.

Mr. JOHNSON OF OHIO. OK. Well, thank you. Madam Chair, my time has expired. I yield back.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Loeb sack, 5 minutes.

Mr. LOEBSACK. Thank you, Madam Chair.

This has been absolutely fascinating. Very complex stuff, very difficult for the average person. A lot of—and those of us up here on the dais who deal with these issues, very difficult to deal with on a day-to-day basis and to understand the issues. I am going to have a couple of questions in just a second having to do with that, but I do appreciate the different approaches that have been taken here.

You know, the more technical issues, not to call you a Pollyanna or something, Mr. Johnson, but this whole idea of interagency cooperation sounds really great. I don't know how likely it is that we are going to be very successful in that front, but I think it is great. Keep pushing that as hard as you possibly can, that what good Government is all about often is the agencies trying to cooperate with one another, even if it doesn't happen very often.

And, Ms. Sacks, I appreciate your comments about policy. I don't think any of us wants to be, you know, a mercantilistic nation either, the way China and a number of others are, but at the same time, for security reasons, we have to be very careful. We have to have industries in America that build these components, that are

part of the supply chain, and it has got to be, I think, much more than it is at the moment.

We are still going to have national security concerns, there is no doubt about that. But the whole idea of risk management makes a lot of sense but, you know, how we are going to be able to identify all these different companies and all the different components and all the rest to go through that, it is going to be a huge challenge, there's no doubt about it.

To me, I just—for me, I just want to know what my constituents can do on a day-to-day basis to deal with all this. Because very few of them are watching this, if we are being covered on any of the C-SPAN channels. And even if they are, it is hard for them to decipher all of the information that we are hearing today.

You know, average folks out there, they have got something in their pocket that they have to worry about when it comes to cybersecurity. And all the information that they have, they have stored and that is available to the bad guys out there. I do—

Before I ask you this, sir, what they ought to do, I do want to say this one more thing, and that is, I was on the Armed Services Committee for 8 years, so—and dealt a lot with sort of how we stay ahead of the bad guys in other countries. And this kind of reminds me of dealing with folks who were working on IEDs on a regular basis, trying to stay ahead of the game. That is what they are trying to do is stay ahead of the bad guys so that they didn't hurt our soldiers, our troops in the field. This is kind of the same sort of thing, how do we stay ahead of the game? You know, because there are a lot of bad guys out there trying to do terrible things to our country when it comes to cybersecurity.

But to bring it down to the level of my constituents, what can these folks do right now who have a concern about this issue, someone who has got an iPhone in their pocket or whatever? What would you recommend that they do today to try to deal with this situation? All of you, please.

Dr. CLANCY. Sir, my perspective is you have to look at the risks that they face. For the most part, the average citizen is facing a criminal, an aspect of organized crime looking to steal their credit card number's identity. They are probably not the target of advanced persistent threats developed by nation-state actors or complex supply chain operations against their personal electronic devices.

Mr. LOEBSACK. Although they may be collateral damage from that.

Dr. CLANCY. They could be, but you have to then look at how those actors would take advantage of that information. So best advice for the average citizen is really to focus on cyber hygiene. The biggest risk to their security is clicking that link in an email that takes them to a Web site where they type in their credit card number. So basic education and cyber hygiene is, I think, the most important thing that the average citizen can do in this space.

Mr. LOEBSACK. Ms. Sacks, I know you deal with the macro policy issues, but—

Ms. SACKS. I agree with Dr. Clancy's remarks. I defer to the security experts on this.

Mr. LOEBSACK. Thank you.

And, Mr. Johnson.

Mr. JOHNSON. And I think simple awareness is a very big first step, whether it is online activity or purchasing devices. Asking the question of whether I am doing this in a secure way actually will usually lead you to the right secure step.

Mr. LOEBSACK. Where can they find information to help educate them about this? Where can they go?

Mr. JOHNSON. There are a number of resources through the Government, through NIST publications, NTIA, FTC, FCC, DHS. And I think we are at a point now, and this is where the imperative of a coordinated, integrated Government operation is so important, because consumers need to know where do I look. They shouldn't have to look in a variety of different places.

Mr. LOEBSACK. I think it is our job too as Members of Congress to get that information out to our constituents as well. So thanks to all of you. My time is up. I appreciate it.

And I yield back. Thank you, Madam Chair.

Mrs. BLACKBURN. Mr. Kinzinger, you are recognized.

Mr. KINZINGER. Thank you, Madam Chair, for this important hearing, and thank you all for being here. I think it is an important nexus between national security and E&C that, unfortunately, I don't think a lot of people see. So I appreciate it.

Dr. Clancy, I appreciate your service at the NSA. I fly for the Air National Guard. I do mostly ISR missions, so you can make that link there. I have become concerned recently about these reports of Stingrays and cell-site simulators popping up around Washington, DC, which has made it into the open source. Are you aware of reports that DHS has detected the presence of these devices in the greater DC area?

Dr. CLANCY. I certainly have seen the volley of letters back and forth between Congress and the FCC on the topic. There have been a number of academic studies as well that have identified the likely presence of such devices in the area as well.

Mr. KINZINGER. So DHS has confirmed that they have detected their presence, but they said they can't physically locate the Stingrays. We have consulted with industry to figure out, you know, what industry can do to help.

In the initial meeting, they told us they had met with the National Protection and Programs Directorate on the matter and they confirmed their awareness of Stingrays, but NPPD doesn't seem to know everything they need to know to actually do something about them. While protecting, of course, sources and methods, do you think they are obligated to share some of this intelligence with industry under the Cybersecurity Act of 2015?

Dr. CLANCY. I think that there are a variety of ways to detect Stingrays. I think—and I am using Stingrays as a generic term to reflect NG capture technology in general. I think that 5G standards have introduced new portions within the standards that will allow carriers to be able to detect the presence of rogue-based stations. And I think we are all excited about that capability as a way for sort of a network-centric approach to addressing that problem.

I think that there are a lot of sensitivities around the technology, given its origins, and that has made it difficult for effective information sharing between people that might seek to police this activ-

ity and those that are technical experts on the underlying technology, although I am not in a position to, I guess, have an opinion about whether the Cybersecurity Information Sharing Act is the appropriate form for that information exchange.

Mr. KINZINGER. And my concern is, you know, not from a certain use perspective, but from, you know, this idea that there may be intelligence agencies in the United States or in DC specifically, which we have read about in open source, that are actually doing this. And that is a big concern, because I would think if in fact there are foreign intelligence agencies using this technology, that should be a high priority for us in terms of determining that.

Like you, I understand, you know, the sensitivity of talking about it, because, you know, it is what it is. We have reached out for more information, so we will follow through on that.

To Mr. Johnson, the House Armed Services Committee marked up the fiscal year 2019 National Defense Authorization Act. It included a blanket ban on Huawei and ZTE equipment by Government agencies. I was very surprised and, frankly, concerned by the President's comments recently, in fact, showing somehow a loosening up of that concern with ZTE. And I hope they were comments that were misinterpreted or at least there is some other thought given to that, because national security is my top priority in Congress. In a perfect world, I would like to see a strong security posture on this front with zero industry impact, but I feel like that is fairly unrealistic.

Is there a way to achieve a strong national security posture, including removal of corrupted equipment, with a relatively low impact on industry? And could any impact be distributed over the long term to minimize industry compliance costs?

Mr. JOHNSON. I do—I think so. And I think the way to do this is sort of there are three issues that are key to keep in mind. One is these issues are very, very complex and they touch a number of different areas. And so it is very important to get this right and that we use precise instruments instead of blunt instruments where possible.

Two is that three companies have been identified in statute and in other Government actions—one Russian company and two Chinese companies—and they have been identified for a number of reasons that we could just—the number of public reasons and a number of reasons that we could discuss in a SCIF. And the FCC proposal on these issues is going to be an important beginning in fleshing this out.

The third thing is that we need a process that I would say is much like how after World War II the Goldwater-Nichols Act brought together all the different services and created a joint interoperable military, and is something I know you can appreciate. And that type of approach, it is very difficult to do. In the case of the military, it took a long time. We need that type of effort for not only the Federal interagency, not only the Federal interagency and the independent regulatory agencies, but also the Government and the private sector. It is going to take a long time, but we are a lot further along than we were I would say 10 years ago when we first started looking at these issues and literally none of the players knew what the other ones were doing or how to do it.

So we need to get to the point where we can act quickly and deliberately and know that we are taking sure-footed steps that consider all the holistic elements.

Mr. KINZINGER. Thank you all for being here.

And I thank the Chair for her latitude. I yield back.

Mrs. BLACKBURN. Absolutely.

Ms. Eshoo, you are recognized for 5 minutes.

Ms. ESHOO. Thank you, Madam Chairwoman, for having this important hearing. And thank you to the witnesses for your testimony.

This is an issue that I go way back on. I was a member of the House Intelligence Committee for almost a decade, and the issue of Huawei and the challenges that it represented I took very, very seriously. And as a matter of fact, when I was leaving the committee, and Mike Rogers, a former colleague and then chairman of HPSCI, I made him swear on a stack of Bibles that he would pick up the baton and keep going on this. Why? Because when our country was attacked on September 11, there was one thing that we had that worked and aided us in our national security, and that was our telecommunications sector. That is where the gold was.

And, you know, for us to be examining this now is very important, but we are not starting from scratch. It is a completely different picture now in terms of sophistication in our systems, what is manufactured, what companies know, what other companies have, what they do, how effective they are, who they buy from. And so I think that the Congress has the tools to make a very strong decision. Mr. Kinzinger said that he takes national security as his top issue. It is the top responsibility for every single Member of Congress. We take our oath of office to protect and defend, enemies external or internal. So we cannot afford, the United States of America cannot afford to play footsie with these companies. They represent a direct challenge to our national security.

So what I want to ask you is, have any of you done an analysis of the costs of whatever it takes in terms of the—you know, a trusted supply chain so that we can make the shift and we don't have to bother or be bothered with ZTE or Huawei or anyone else that presents themselves down the road? Whomever wants to answer. Has there been any kind of cost analysis of this?

Ms. SACKS. I say this having worked in the national security and the Department of Defense community, there has not been public information released about the specific problems associated with Huawei and ZTE. I am not saying they doesn't exist, but in order to conduct exactly that kind of assessment, to do the kind of—

Ms. ESHOO. But we know—let me interrupt you just a second.

Ms. SACKS [continuing]. Needs to have public information, it cannot be classified—

Ms. ESHOO. Just a second. I know from classified briefings what the challenges are. I am not asking you to tell me about that. I already know that. The challenge is, we want to have a system where we are not reliant on them for anything, for anything. And I think in different ways, you all have maybe touched on it or gone around it. So would you like to say something on this?

Mr. JOHNSON. Yes, ma'am. I think we need to urgently start that process. And all the pieces are in place now, we know a lot more about what needs to be done.

Ms. ESHOO. So there has not been this examination, as far as you know?

Mr. JOHNSON. I think we are behind in doing that analysis, but these processes that are underway right now are—will flesh this information out. But, no, I think we don't know enough about—we need a record on this. And that is what is so valuable about this FCC process. It is focusing on one element of the problem, but it is the very first public record that will exist on this issue.

Ms. ESHOO. I thank you.

Madam Chairwoman, I think that our committee needs to do a letter to the administration. I am not saying this to be political. This is a national security issue, and Republicans and Democrats have taken, both at this committee, at the House Intelligence Committee, for years have weighed in relative to these companies and the national security threat. I don't know what is happening. I think that the Secretary of Commerce certainly did the right thing. We should do this on a bipartisan basis. I don't know what is taking the President in whatever direction. I am not going to make any political hits on it. Overall, it is wrong and it is dangerous for us. And I think that the Congress, coequal branch of Government, should weigh in with the administration formally and say, "This is not the way to go."

So I would just request that and have you consider it. I think there would be support from this side of the aisle, and I think there would be from yours, as well.

So I want to thank the witnesses and for your patience. I have gone over my time. Thank you for your testimony on this most important topic.

Mrs. BLACKBURN. The gentlelady yields back. And I look forward to discussing with her how we can continue to work in a bipartisan manner on this.

Mr. Bilirakis, you are recognized for 5 minutes.

Mr. BILIRAKIS. Thank you. Thank you, Madam Chair. I appreciate it very much.

Dr. Clancy, one of your recommendations to strengthen the supply chain is a collaboration between industry and Government to identify at-risk products. That information can then be shared with developers and suppliers. The Department of Defense uses a software process standard called common criteria in which software is penetration tested for vulnerabilities and then assigned a certification grade. The FAA has a similar process for its flight control systems.

I recently met with a software company with a cybersecurity research facility in my district. The company suggested a similar process at risk management—of risk management for medical devices and other sensitive IoT devices. The results could be used to identify and mitigate security threats. Interestingly, because it is a process and not a regulatory standard, it can evolve with new technologies and threats.

So, Dr. Clancy, is this something that aligns with your thoughts on Government collaboration? And can you expand on any other

ideas you have for Government participation in this space that does not involve quickly outdated standards?

Dr. CLANCY. Certainly. I think the common criteria is a great example of a framework that looks at cybersecurity risks, specifically with software as you point out. There are—I think you could more broadly look at the NIST cybersecurity framework as capturing kind of a superset of those objectives. I don't know that any of them are necessarily well suited or have been applied in the supply chain space yet. I think that is something that is a study that would need to be undertaken.

I think in terms of managing and governing that process, I think the interagency approach that Mr. Johnson proposed is a great starting point for that. The knowledge of the threat is distributed across many different Government agencies. And I think they would need to come together in order to bring together that complete picture in order to collaborate with industry effectively.

Mr. BILIRAKIS. Thank you.

Mr. Johnson and Dr. Clancy, this question is for both of you. There may be times where specific telecom suppliers raise truly serious concerns which warrant action, but we cannot avoid the reality of today's global supply chain. Where do we stand if we cannot adequately respond to threats that arise out of such a global supply chain? We will go with Mr. Johnson first, please.

Mr. JOHNSON. I understand your question is, given the interconnected complex nature of the global supply chain, how do we identify particular threats?

Mr. BILIRAKIS. Yes.

Mr. JOHNSON. I think just borrowing on some of my fellow witnesses' testimony, taking a risk management approach is crucial, as is clear guidance to the market about where the risks are, and that could include individual companies, it could include individual products of individual companies, or it include other things that we haven't identified yet. And I think the most important thing is to look at this through—not through a stovepipe of a certain agency or a certain industry sector, but holistically through the entire market in all its complexity, and clearly provide private sector advice or guidance about where the risks are. And this process needs to include their take on it, where do they see the risk and where do they see—what do they see as how to do supply chain risk management and trust its suppliers, and then create the positive feedback loop that continues to inform the market about what is good and what is trusted and what is not.

Mr. BILIRAKIS. Dr. Clancy, please.

Dr. CLANCY. As I pointed out in my testimony, I think it is going to be impossible to eliminate all risk from the supply chain. It is too global and there is too many different ways that every product touches that global supply chain. So, again, risk management is critical. You have to pick the areas where there is the most risk in terms of bad actor behavior and the areas where there is the most criticality in terms of our critical infrastructure and start there and then work your way down.

Mr. BILIRAKIS. Thank you. Very good.

I yield back, Madam Chair. I appreciate it.

Mrs. BLACKBURN. Mrs. Dingell, you are recognized.

Mrs. DINGELL. Thank you, Madam Chairman.

Much of the confusion surrounding this issue relates to the simple truths that we don't know the full scope of the problem. And although it is helpful to hear different ideas for mitigating risk across networks, I believe it is difficult to create effective policy without knowing what we are up against. It is difficult to change, or in this case, protect what you can't measure.

These questions are all going to be for Mr. Johnson.

Mr. Johnson, you say in your testimony that you advise companies trying to navigate these threats. Can you tell us, generally, whether companies in the private sector are beginning to take some sort of inventory of the risks that they are facing?

Mr. JOHNSON. I do think—and I have worked with a number of the companies in this sector speaking broadly throughout in the communication sector device, cloud, and internet infrastructure. For about a dozen years in, I don't know if I can't hold a job, but I think this is now my fifth different job that I have worked with a number of these companies in both in Government and now in private practice. And I can say two things: Number one, it is core to their business to—to their business imperatives as a bottom line institution to advance supply chain security.

And number two, we as a collective Government and industry partnership have advanced pretty significantly in those dozen years in terms of situational awareness. We are not where we need to be, and I don't think any individual company or any individual agency is, but we have come a long way and the trajectory is where it needs—is headed in the right direction. And I think now we just need to step on the gas with some urgency to fill out the data that we don't have.

Mrs. DINGELL. So are there models for conducting this sort of dynamic threat assessment that stakeholders should be looking to?

Mr. JOHNSON. I mentioned this briefly earlier. There is a model in the last year that has—of a process that has just been completed that I really think is a model of cybersecurity policymaking. It was conducted under the executive order to reduce botnets and other distributed automated threats. It was led by the Commerce Department and the Department of Homeland Security, but included input from a whole host of other agencies and the FTC and the FCC and most crucially was driven by private sector input.

So the companies that are out on the front lines were helping drive this process that was convened by the Government. And I think that model, it was very robust, it was very busy, there was lots of activity, there were lots of threads that were being followed, but it was navigable and it was clear. And I think that type of model could be replicated on the supply chain side, along with legal mechanisms to ensure the confidentiality of sensitive data that is exchanged.

Mrs. DINGELL. So on the Government side, how could Federal agencies best situate themselves to be effective partners for the private sector? Do you think that the FCC, the Department of Homeland Security, Commerce, each have a role to play?

Mr. JOHNSON. I do. I think they and as well as a number of others do. In the case of these issues, I think the Department of Homeland Security is the sector-specific agency for the communica-

tions sector and the IT sector so they can—they should probably—and they also administer the statutory protections for protecting confidentiality. I think they can sort of be the lead cat herder in the interagency and in convening this process, but certainly the Department of Commerce, both through NIST and NTIA, and the International Trade Administration and the Bureau of Industry and Security, have very important perspectives to add, as does the intelligence community, Department of Defense, and other regulatory agencies.

Mrs. DINGELL. So, finally, what should the Federal Government be doing to incentivize research here at home so that many of these emerging technologies are built here and developed here?

Mr. JOHNSON. I think really the—that is a—that is maybe the most difficult question of all, because we don't—here we don't do State-directed, industrial policy like China does, and I don't think we want to do that. But we also want to send a very clear message to the market that the future is secure. The future of the market needs to be trusted suppliers and secure products and services.

And I think that maybe the biggest benefit of these processes that are taking place right now is it sends a pretty clear message that security is—needs to be the future of the market. And if you build it secure, you are going to benefit in the market.

Mrs. DINGELL. Thank you, Madam Chair.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Lance, you are recognized.

Mr. LANCE. Thank you, Chairman. To the entire panel, ensuring a secure supply chain is a priority for all of us, but the real question, from my perspective, is how do we as policymakers, and we certainly don't have your expertise, ensure that we get it right and avoid unintended consequences?

For instance, we saw the Department of Commerce crack down on ZTE and rightfully so for violating sanctions in Iran and North Korea, and it is essentially an arm of Chinese intelligence. However, Commerce's penalties against ZTE also meant companies are not sending security updates to those phones. While we are trying to protect ourselves, we are also potentially leaving ourselves vulnerable.

In your judgment, the expertise of the panel, how do we strike a balance and protect ourselves from bad actors like ZTE without opening up other security gaps? I will start with you, Dr. Clancy.

Dr. CLANCY. So I think your example around software updates is a great one. If we look at—again, if we look at the problem holistically and you seek to manage cyber risk for an entire industry, that includes both the selection of equipment and the configuration, provisioning, and management of that equipment. So, for example, you can trade off whether or not the relative risk associated with a low-cost component that is—perhaps has its software update patch path blocked because of some of these requirements, and compare that to potentially a more expensive piece of equipment that doesn't have that.

So, again, if you are looking at the overall risk management, I think you would be able to make those trades and be able to make the best decision for overall security of, in this case, telecommunications critical infrastructure sector.

Mr. LANCE. Thank you.

Ms. Sacks.

Ms. SACKS. I agree with Dr. Clancy. I think this needs to be a risk-based approach that is granular, that looks at specific equipment and components going into systems not just for companies of certain countries, but for all equipment providers.

Mr. LANCE. Thank you.

Mr. Johnson.

Mr. JOHNSON. Yes, sir. I think we need to find maybe not the balance, but the combination between deliberate action and expeditious action. And I think there is a way to do that even in this scenario. It needs to be clear. It needs to be—the steps and timeframes or their phaseout periods, that all needs to be determined and it needs to be clear to the consumer and the companies who are out on the front lines about what is going to happen and when.

Mr. LANCE. Thank you.

Ms. Sacks, in your testimony, you recommended that the United States look for leverage to change Beijing's behavior and its ICT policies, and that it is not in our best interest to act unilaterally.

Have other countries taken action against ZTE and Huawei? And should the U.S. be looking to leverage the ZTE situation to pressure China on its ICT policies instead of as a trade bargaining chip?

Ms. SACKS. Two points on that: One model that is worth considering is the U.K., which has incorporated Huawei into their systems, has set up a security testing center which they use to test Huawei equipment that goes into the network. It is independently audited and the results are reported directly to the National Security Adviser.

So that is one model that should be considered, although we need to take a number of things into consideration to strengthen it. That center is staffed entirely by Huawei employees. I think we would need a much more strengthened version in the United States. And particularly if we are thinking about 5G and the complexities around massive software involved with 5G, would that kind of model be adequate for the new security challenges posed by that.

So that is just one example of another country that we might want to take into consideration.

Mr. LANCE. In your professional judgment, is the U.K. the best at this in the world?

Ms. SACKS. I don't know if they are the best, but they are the one—I think that their model is one which is worth studying.

Mr. LANCE. Thank you. This has been a very interesting panel, and I thank all of you for participating.

And, Chairman, I yield back half a minute.

Mrs. BLACKBURN. The gentleman yields back.

Ms. Matsui, you are recognized.

Ms. MATSUI. Thank you, Madam Chairman, and thank the witnesses for being here today.

Virtual private networks assist companies and businesses in preventing foreign governments from monitoring traffic between providers and their devices. There seems to be ongoing uncertainty surrounding whether and how rules blocking the use of VPNs in China not approved by Chinese government will be implemented.

Ms. Sacks, as you note, this review requirement has a practical effect of allowing the Chinese government to approve the channels companies use for international connectivity. What security threats arise in China monitoring, reviewing, and approving VPNs, especially communications using VPNs where Huawei and ZTE have installed network equipment?

Ms. SACKS. One of the most important areas that we should watch are restrictions around corporate VPNs in China, not just for consumers, but also for companies in terms of sending information across borders to conduct HR baseline financial operations needed to conduct business there. I think that there are a number of channels that the Chinese government is using to increase their ability to monitor and control networks, the data, the information that flows across that. The VPNs is one.

There are multiple different kinds of security reviews that are all in process. The scope of them is not clear, and there is competing jurisdictions, even within these different kinds of reviews. So you have the multilevel protection scheme, which has been in place for several years, but now you have a new review of network products and services connected with critical information infrastructure operators in China. We don't know what is going to follow the scope of that.

Ms. MATSUI. OK. Well, thank you.

Back doors into hardware and network components are designed to avoid detection, and vulnerabilities introduced at the beginning of the development process in the supply chain are particularly hard to detect. I echo the concerns of my colleagues over the national security threats posed by equipment providers to the integrity of the communication supply chain. I understand inherent difficulty approving where there isn't a back door into our networks.

I want to ask this of each of you. Do you believe sufficient work is going towards a process to ensure when there is or is not a back door in switches, routers, or other networking equipment? Dr. Clancy?

Dr. CLANCY. As you point out that such back doors or intentional vulnerabilities in software are extremely difficult to detect, particularly if they are specifically seeking to be hidden. I think that it would be very challenging to do a thorough assessment, for example, without access to source code for the presence of such vulnerabilities in equipment purchased from foreign vendors. I think that that, though, is—the bigger threat, at least immediately though, is the more front door access, which is the managed vendor access where they are explicitly given access to the license for the purpose of management.

So I think we need to tackle the front door first. The back door is I think something that will only be effectively tackled through a risk-based approach, because guaranteeing that there are no back doors is virtually impossible.

Ms. MATSUI. OK. Ms. Sacks, do you agree?

Ms. SACKS. I don't have anything to add to that.

Ms. MATSUI. OK. Mr. Johnson.

Mr. JOHNSON. Yes, ma'am. I agree with what Dr. Clancy said about the difficulty of finding the purposely in place back door and

also the threat of the front door that we see right now through vendor management.

And Ms. Sacks had a really great example of an innovative approach to this that the U.K. is taking with regard to Huawei. The only thing I would add to that is that at the same time that the U.K. decided to that, we in the United States were—those proposals were being made in the United States as well. Let us do this, we will do an independent testing, et cetera, and the United States decided not to do that. And I think that is probably—while I think it is correct that the U.K. model is a very valuable reference point for testing, I am very weary of the capabilities of testing to be able to find the real problems when you have such a sophisticated actor. So I might—I just think testing can be an important part of it, but it is never going to be a wholly sufficient answer. And I think we need testing along with a holistic approach to trusted suppliers.

Ms. MATSUI. All right, OK. It looks like I don't have enough time. So anyway, I yield back the balance of my time. Thank you.

Mrs. BLACKBURN. The gentlelady yields back.

Mr. Guthrie.

Mr. GUTHRIE. Thank you, Madam Chairman.

I appreciate the opportunity to be here and for our witnesses to be here today for a timely issue.

My first question is for Ms. Sacks. It appears the response to network threats so far have been tactical with regard to specific threats and strategic with regard to competition in the supply chain. So what can we do to ensure our response is proactive and coordinated across the Federal Government? And do we need to formalize this approach? And if so, what sort of framework is needed?

Ms. SACKS. I think that there has been a conflation of a lot of different kinds of challenges and problems connected to Chinese security and industrial policy threats, and we need to be much clearer. Are we talking about export controls, national security risks, IP theft, FCPA, and that will help enhance coordination, better coordination among these different actors given the different types of issues at hand. And once we are able to do that, I think that we can work more effectively with our allies and partners in other parts of the world to exert the kind of leverage needed to change behavior.

Mr. GUTHRIE. Do you have any thoughts of what agencies, timelines, and what scope, and how we balance agility with thoroughness?

Ms. SACKS. Here I think I would defer to Mr. Johnson.

Mr. GUTHRIE. That is fine. I was going to ask him next. I was going to ask him next, so there we go.

Mr. JOHNSON. I spend a lot of time pushing that boulder over the mountain in the interagency. As I said a little bit earlier—

Mr. GUTHRIE. Didn't roll back down, did it?

Mr. JOHNSON. It rolls back down, and you push it a little bit further and it rolls back down again.

But there has been a lot of progress made in the past decade or so in terms of getting the team to be more of a well-oiled machine. It is not that yet. But I think we have ways to—we don't need to find ways, we have ways to have a coherent, holistic process that

includes input from all the relevant stakeholders in Government and also in the private sector. That is what we need to do as—it needs to be—we need to be in a big hurry about it, and it needs to be urgent, and it also needs to be deliberative and continuous. We are not going to finish this project. It is going to go on for as long as we have these capabilities.

Mr. GUTHRIE. OK. So Mr. Johnson talked about the agencies. So, Dr. Clancy, or any of you, actually—and you did mention it has got to have input from the private sector. So what road should the private sector—I will ask Dr. Clancy first, then we can move on, what road should the private sector play in collaboration with the Federal Government to address the telecom supply chain risk assessment from the manufacturing perspective?

Dr. CLANCY. Well, I think I will highlight a point I think that is been made earlier in this hearing, is that the Cybersecurity Information Sharing Act, landmark legislation, really enables tactical sharing of operational cyber threat data between the Federal Government and industry. I think over the last 3 years as that has been operationalized, we have seen a lot of industries come together and effectively use those instruments.

Mr. GUTHRIE. Well, passing that was actually kind of controversial. I mean, some people really opposed that, and Members. I mean, so how has that been effective? I didn't think about that, you just said it, but—

Dr. CLANCY. So I think it has—we have seen many of the ISACs, the industry specific information sharing entities adopt various technology standards, like STIX and TAXII, protocols that are specifically designed to share real-time threat information. I think there is still lots of hurdles to go. I think there are lots of parts of industry that are still nervous about sharing information that might be negatively viewed by their regulators, and so I think there is still some caution from an industry perspective. I think they are enjoying the ability to consume information from the Federal Government, though. So we haven't, I think, seen full bidirectional sharing between industry and Government, but we are getting a lot closer to that, in my personal opinion.

But as you project that forward and you look at supply chains, supply chains are a very different type of threat. It is not an operational tactical threat. It is a much more strategic threat where the long game is being played by adversaries in this space. And so it is less about tactical information sharing but more about understanding the bigger picture and being able to share risk assessments associated with that with industry and among members of industry and with Government. I think we haven't gotten that far yet. And I think that would be, again, whether it is the interagency framework that Mr. Johnson has proposed or other mechanisms, I think that is really the next frontier.

Mr. GUTHRIE. I see you nodding, Mr. Johnson. Any comment you want to add to that?

Mr. JOHNSON. I think that is right. The next step—we talked about this right in the beginning, the next step beyond the tactical real-time information sharing of the Cyber Information Sharing Act is a more deliberative, in many cases, human interface about longer term strategic threats, and companies will need to have cer-

tainty that going into talk to the Government about what they are worried about doesn't come back and hit them. You might call it a reverse Miranda protection where nothing I say here will be used against me. And we really need to build this team and pull it together, and it has to be a trusted environment. There are some—the PCII protections are statutory protections that provide that. And I would be delighted to talk with you more about that when I am not over time.

Mr. GUTHRIE. My time has expired. I appreciate it. Thank you.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Butterfield, you are recognized.

Mr. BUTTERFIELD. Thank you very much, Madam Chair.

Good morning to our witnesses today, and thank you for your testimony.

Madam Chair, in thinking about the hearing today and trying to get a few notes ready to talk to these witnesses, it became pretty clear to me how difficult securing our supply chain will be. This seems not to just be a national security issue, but a technological issue, an economic development issue, a consumer issue, and even a trade issue. And so I appreciate that our colleagues on the Armed Services Committee understand how to approach the national security portion, but we must also strive to better grasp the broader ramifications.

And so, Mr. Johnson, in your written testimony, you note that securing our chain raises complex national security, strategic, economic, business, and technological concerns. So my question, sir, to you is, to ensure that we have developed the right policy to manage the risk to our chain, supply chain, do you think that we, Congress, should take steps to ensure we are adequately thinking through each of these complexities?

Mr. JOHNSON. Absolutely, yes.

Mr. BUTTERFIELD. In their interrelationships.

Mr. JOHNSON. Absolutely, yes. This is a very big deal and we need to get it right.

Mr. BUTTERFIELD. What are some of the economic, business, and technological concerns that we should be focused on in their intersectionality?

Mr. JOHNSON. Well, just to take the example of 5G deployment, the issues that pertain to 5G deployment moving to an almost entirely connected world, really have—in some ways they have all the elements of what our country went through in the fifties and sixties with regard to the space race. The implications of what types of companies and what types of countries are ahead in deploying 5G have geostrategic implications, they have economic competitiveness implications, they have espionage and sabotage and warfare implications. And so we certainly want the United States and other rule of law based market democracies and those companies to be in the lead in order to maintain the interests that we—and values that we hold dear.

Mr. BUTTERFIELD. Now, there are some conversations that we have heard about outright banning equipment from China, and I am paraphrasing some of that. I don't suspect that is your view. But what impact would outright banning equipment from China have on low-income consumers?

Mr. JOHNSON. I think this has been expressed earlier by my fellow witnesses, but I think a country-of-origin ban of any kind is too blunt of an instrument, and it is not necessarily feasible in the world we live in now, particularly with regard to China. There are a lot of trusted suppliers that have elements of China in their supply chains. And so we need to take more of a scalpel and identify bad actors.

With regard to the bad actors that have been identified from China, and certainly there are some China-specific concerns that we need to raise, but with regard to the two Chinese companies that have been identified, the record that is being built in the FCC through the proposal to prevent USF funds from going to companies like that is going to flesh out what the effect in the market is and, very importantly, what the effect in the lower income and rural markets are where companies like Huawei and ZTE have most of their U.S. presence.

Mr. BUTTERFIELD. Let me ask you this, does the draft defense authorization legislation that has been put forward accurately take each of your concerns into account?

Mr. JOHNSON. I think that—any proposal, particularly one that is embedded in statute, needs to have a very significant vetting, tire kicking, and make sure that, you know, through hearings like this, that all of the important elements and considerations are embedded in whatever statute becomes law.

Mr. BUTTERFIELD. Dr. Clancy, you have 30 seconds, my last 30 seconds. Any comments on any of this?

Dr. CLANCY. So specifically with respect to your last question, I think the—while certainly the actors that have been identified so far represent, I think, substantiated risks to national security, they may not be the only ones, so focusing only on those two is I think one challenge. I think the other aspect that needs to be addressed is, again, the criticality. There is a difference between a phone and a core network router, and that is not adequately reflected in the current draft legislation, in my opinion.

Mr. BUTTERFIELD. Thank you.

Sorry, Ms. Sacks, but we ran out of time.

I yield back, Madam Chair.

Mrs. BLACKBURN. The gentleman yields back.

Mr. Long, you are recognized.

Mr. LONG. Thank you, Chairman.

Dr. Clancy, due to the interconnected nature of telecommunications networks, operators don't always have visibility into other parts of the network to know whether there may be vulnerabilities. In some cases, information may be carried over the network that has ridden over foreign networks. Can you speak to the global nature of the internet and how we should address vulnerabilities given these threats?

Dr. CLANCY. So there are a whole range of potential global threats to the internet itself. The internet, from a government's perspective, is really a series of bilateral contracts between internet service providers that stitch together to form the fabric of what we know the internet to be. And any of the components of that core infrastructure have the ability to influence things like control playing aspects of the internet, routing tables being the most notable

example, or any major internet service provider can cause major damage to the internet by virtue of how the internet is constructed. So I think that there are a whole range of threats.

I think the larger the market share of any one particular vendor, particularly vendors that we deem as a national security risk, increases the global exposure to that risk, to that threat.

Mr. LONG. OK, thank you.

And, Ms. Sacks, the Department of Commerce denial order issued against ZTE is commonly cited as one of the reasons ZTE sought to cease operations in the United States. This order, a law enforcement action resulting from the violation of sanctions terms, was very disruptive. If this disruption serves as a model for future bans on specific network or device equipment providers, what is the impact on our ability to remain globally competitive?

Ms. SACKS. ZTE clearly violated export controls, and this is an export control issue rather than a trade issue, although there are also separate national security implications. It has not been usual for bans on sanctions to be lifted, but the timing and the process involved with ZTE was highly unusual. We need to see what comes out of this. U.S. companies are definitely going to have impact from that ban. We need to see what happens in terms of the President's moves as he works to negotiate with the Chinese, but the conflation of an export control issue with a trade issue is worrisome in my mind.

Mr. LONG. Are these sorts of bans effective or are there other proactive measures that we can take to protect our networks and compete globally?

Ms. SACKS. We have seen with Beijing that access to global markets is a point of leverage that has brought them to the negotiating table in 2015, so ahead of Xi Jinping's visit where they came with up the cyber agreement. So we see that access to global markets is a point of leverage. However, we need to also consider the ramifications on the follow-on effects in terms of retaliation against U.S. companies. That is why it is important to work in a multilateral fashion on this.

Mr. LONG. OK, thank you.

And, Madam Chairman, I would like to submit an article for the record, "US Army base removes Chinese made surveillance cameras." This is Fort Leonard Wood in my home State of Missouri.

And with that, I yield.

Mrs. BLACKBURN. Without objection. The gentleman yields back. [The information appears at the conclusion of the hearing.]

Mrs. BLACKBURN. Mr. Costello, you are recognized.

Mr. COSTELLO. Thank you, Madam Chair.

Mr. Johnson, how would you advise a telecommunications provider when it is making plans to expand its network? Of course, providers want to be cost conscious and purchase economical equipment, but they also want to make sure they are not introducing vulnerabilities into their network. How do these providers weigh the tradeoffs in making these decisions?

Mr. JOHNSON. I think that is one of the central questions, sir. And it depends on who the provider is. I think most of the large providers are aware of and can take other options than some of the companies that have been identified as particular concern.

With smaller providers who operate on much smaller margins, it becomes a much more difficult question. And I think according to our—you know, according to the public record from our Government and the intelligence community, that has been part of the reason why we are concerned about Huawei and ZTE in particular, because the Chinese government knows that, the companies knows that, and so they can undercut the price. And you hear anecdotes about the company sales approach is essentially tell me what your lowest competitor's price is and I will undercut it.

Mr. COSTELLO. And let's talk about rural providers. How do we mitigate the risk to come along with that equipment, equipment obviously purchased at below market rates? Is there a risk that if we ban certain types of equipment, it will increase the cost or time for expanding broadband access?

Mr. JOHNSON. I think there is a risk of a disruption, and that is why I think this process needs to take place very deliberately and expeditiously. It needs to have clear guidance to the players about what is going to happen when, what they need to do, what they need to be aware of. And any disruption should be dealt with through that process. But I do think—I have got some faith in the fact that there are lots of other competitors who would love to keep competing in a competitive market and not essentially be frozen out of certain parts of the market by uncompetitive, undercutting of prices.

So I think that if those two companies are restricted in some way from certain parts of the market, I am very confident that the market will respond, it will send a signal to other players in the market that, hey, there is reason to play here, because you are not going to be undercut in an uncompetitive way. And if there are any vacuums, they will be quickly filled.

Mr. COSTELLO. So far we have been able to successfully limit our risk by managing the standards bodies. Is this method sustainable? And I will ask an ancillary question, is leveraging the transparency aspect of standards bodies enough or can nefarious actors still engineer proprietary technologies but introduce threats to the networks while still complying with the agreed-upon standard?

Mr. JOHNSON. That is a great question. I will say a piece and then defer to Dr. Clancy, who is an expert on these issues. But the sort of soft power of shaping the standards environment is something that is very important, something that the United States has really led through its standards approach over the past several decades. And the Chinese have recognized that, and now they are throwing a lot of resources at these standards discussions and standards bodies to help shape the field in such a way that it benefits their products and gives them intellectual property benefits that last a lot longer.

But I will defer to Dr. Clancy because I think he's participated in this process.

Dr. CLANCY. I would agree. I believe that—my observation of China's role on standards bodies has been primarily that they are looking to move their role into the innovation and IP creation, and that is critical to the standards process, away from simply manufacturing devices. And so as they look to sort of professionalize

their telecom ecosystem and be out in front, standards is one of the ways that they are leveraging that.

I do believe in the open and transparent processes in standards, so I am not worried about sort of slipping in back doors in the standards, but there is, as Mr. Johnson noted, sort of this soft power influence in which companies technologies end up getting preferred and written into the standards.

Mr. COSTELLO. Semiconductors and microelectronics have comparative advantage, I think, in standard setting focus. From a securities standpoint, are network operators left at a competitive disadvantage?

Dr. CLANCY. Specifically with respect to their use of—

Mr. COSTELLO. In terms of power in the standard setting bodies.

Dr. CLANCY. So, I mean, in the standard bodies that I have been involved in, it has been basically the more internet Ciscos and Qualcomm and those sorts of companies that are really leading those standards efforts here from the United States. I think that that then translates down into silicon when you go to manufacture the product. I am not sure if quite I understand your question, though.

Mr. COSTELLO. Well, I am out of time, so we will follow up afterwards.

Thank you. I yield back.

Mrs. BLACKBURN. Mr. Walberg, you are recognized.

Mr. WALBERG. Madam Chairman, I thank you for waving me on this subcommittee. It is of real interest, the subject today.

Ms. Sacks, one of the challenges we are talking about in our discussions on domestic manufacturing capability, we are also talking about our ability to identify emerging technologies and bring them to commercialization for both U.S. and global markets. My colleagues today have expressed a need for a national strategy that addresses threats to our telecommunications networks to competition in the supply chain and to national security.

Can you elaborate a bit more on how human capital, those people who know how to do this stuff and can be creative with integrity, plays into such a national strategy?

Ms. SACKS. Human capital is one of the areas in which our technology development process is actually very interconnected with China. We work closely with engineers in China, there are a lot of very highly skilled, talented engineers coming out of China. We have research centers that are highly interconnected. And so this is an area where there are possible national security risks that need to be examined, but we also need to examine what are the economic and the innovation benefits that come from some of that interconnection on human capital. So we should incorporate that into the discussion as well because I think that there are potential downsides and upsides to that level of interconnection.

Mr. WALBERG. What can Congress do to help to lead on this part of the puzzle?

Ms. SACKS. Let me get back to you on that one.

Mr. WALBERG. OK. I take that as an interesting answer and look forward to the answer.

One of the challenges when confronting threats to our supply chain is the truly global nature of today's ICT supply chains. As

vendors that provide potentially vulnerable equipment continue to improve the quality of their products and services and gain global market share, the question is, what can we do to ensure our domestic providers are left with no other option than to procure equipment from these vendors?

Ms. Sacks.

Ms. SACKS. I think that there are three main options, all of which, again, have downsides and are challenging. One is we need to think about investing in ourselves but in a way that doesn't replicate the China model so that we are not leaving it up to the Government to pick winners and losers but enabling R&D and enabling education; an investment in our own companies to be leaders in areas like 5G. We also have to think about what are the software solutions from a mitigation standpoint that we can use, given the fact that there likely are going to be companies like Huawei and ZTE in the global supply chain. And an isolationist approach is not necessarily going to be to our advantage either and could put us in a backwards technology position. So there is a mitigation perspective as well as an investment perspective on our own side.

Mr. WALBERG. So it is not just us building better stuff then, as some would say would be in our best interest.

How does our ability to domestically source our own equipment, though, work in a world where the ICT supply chain is increasingly globalized? And then second question I would ask with that, can you explain how we should take a risk management approach to examining our domestic manufacturing capability?

Ms. SACKS. I think Dr. Clancy has outlined a very effective risk management approach. I will let him elaborate on that.

Dr. CLANCY. Certainly. I mean, I think if you look at domestic products, again, the iPhone which I brought up in my opening statement, the majority of that is sourced internationally. So while we view that as domestic product, very little of the components and the manufacturing itself are domestic. So I think that we need to be cautious to not just look at the company that is selling it to us, selling the end product, but also look at all the pieces behind the curtain that went into manufacturing that as part of an overall risk management approach to supply chain. And that should apply not only to acquisition of Huawei and ZTE equipment from—as part of some network, but also look at the components that would go into the production of a U.S. device as well.

Mr. WALBERG. Thank you. Good advice.

And, Madam Chairman, thank you for letting me wave on, but it is important to understand what assistance we are using, all the parts that are there, but to sure do our level best to make sure that we are secure for all sorts of reasons. So thank you.

I yield back.

Mrs. BLACKBURN. The gentleman yields back.

And as you can see, there are no additional Members who are present and ready to ask questions. So we thank you all for being here.

As we conclude today, I ask unanimous consent to enter the following documents: a letter from Sicuro Innovations, a letter from Commissioner O'Rielly, a U.S.-China Commission report, articles by Sann Sacks and Andrew Hunter of CSIS, two Wall Street Jour-

nal articles, and the ZTE denial order, and one article from The Hill.¹

Without objection, so ordered.

Pursuant to committee rules, I remind Members that they have 10 business days to submit additional questions for the record, and I ask each of you witnesses to respond to those within 10 days of receipt of the questions.

Seeing no further business to come before the subcommittee today, without objection, the subcommittee is adjourned.

[Whereupon, at 12:01 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. ANNA G. ESHOO

Today's hearing on supply chains is about an issue I go very far back on. I served on the House Permanent Select Committee on Intelligence for nearly a decade, and during that time we had close examinations of supply chain manufacturers, including Huawei and other foreign manufacturers, and the serious challenges they represented.

I took these issues seriously more than a decade ago, and I still do today. When my term on HPSCI was ending, I specifically asked the then-chairman, Mike Rogers, to commit to pressing on the threats to our national security that Huawei presented.

When our country was attacked on Sept. 11, 2001, we possessed something that was essential in the age of terrorism—our telecommunications systems. They were and they still are part of the backbone of our national security and intelligence operations.

Fast forward to 2018, when the sophistication of what these technologies can do has increased exponentially, as well as what is manufactured. There is far more that today's companies in this sector on whom we rely for our communications can know, what other companies have access to, and whom they buy from. And we know for a fact, based on years of scrutiny which I was a part of, that certain companies, particularly foreign enterprises, do not have our national interests at heart. Thus, we have no business doing business with them. Period.

Congress can prevent this infiltration of our critical communications systems. The number one responsibility of every Member of Congress is contained in our Oath of Office, 'protect and defend' our citizens from enemies external and internal. We cannot allow foreign entities to compromise our telecommunications sector, because it would create a direct challenge to our national security. I'm bewildered that after so many years of hearings and investigations that we continue to consider whether we should use parts from companies whom we know have adversarial intentions against our country. The answer to this consideration is NO.

¹The U.S.-China Commission report has been retained in committee files and also is available at <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=108301>. The other information appears at the conclusion of the hearing.



Sicuro Innovations LLC

16 May 2018

The Honorable Marsha Blackburn
Chairman
Subcommittee on Communications and
Technology
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Michael F. Doyle
Ranking Member
Subcommittee on Communications and
Technology
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Blackburn and Ranking Member Doyle:

Sicuro Innovations is a cybersecurity firm that has developed embedded and cloud based artificially intelligent (AI) software to secure Internet of Things (IoT) devices in the AgTech, telecommunications, supply chain, and energy industries. Sicuro was founded in response to the absence of security of connected devices integrated into our homes & businesses, and illustrates a critical gap in national security. The deployment of 5G and increased wireless broadband Internet access service presents incredible economic development opportunities including precision agriculture, tele-health, renewable energy, efficient supply chains, industrial manufacturing, and autonomous vehicles. However without an effective government and industry response to the vulnerabilities in our telecommunications networks and their supply chains, we risk losing the ability for smaller companies to compete in a global environment and leave critical nodes of the supply chain and our national security vulnerable to foreign influence.

The American dream is fundamentally based on small businesses' ability to engage and grow within a national and globally competitive landscape. Small businesses need to ensure that everything from the equipment they procure, the broadband service that connects them to the Internet, to the devices that connect to the Internet, are secure. Vulnerabilities in our connected supply chain leave the United States at a competitive disadvantage. Moreover, lack of competition in the vendor market reduces the ability of small businesses to grow and make decisions based on their own safety and security. These businesses need options that not only meet their product and service needs but also options that support our shared investment in our nation's national security. Unfortunately, market pressures have shifted vendor markets against these concerns.

Where we fail to mitigate barriers to competition, we will need an effective strategy to mitigate specific threats to our networks and devices. Sicuro leverages AI to provide small businesses and manufacturers with a secure way to integrate connected devices with 5G. Even in instances where businesses are incentivized to engineer IoT devices with lower quality foreign made components in order to take advantage of "first to market" opportunities, Sicuro can help prevent widespread transfer of malware through IoT and other devices by recognizing anomalies in machine behavior. Though we encourage businesses to use standards bodies to produce and manufacture devices with security in mind, often they are produced with an acceptably poor level of security without possibility of legal repercussion. Even in these instances, Sicuro is one tool that could help mitigate existing threats, and

Page 2

Letter to Chairman Blackburn and Ranking Member Doyle

adapt to threats of the future. We need to take a more proactive and thoughtful approach to the security of our connected environment, rather than simply reacting to the threat landscape as it presents itself and leaving resource limited small businesses with inherently vulnerable devices to take a stand against foreign adversaries and cyber criminals.

I applaud the Chairman and Ranking Member for facilitating this conversation on telecommunications, competitiveness, and national security to ensure the Congress plays an active role in establishing appropriate oversight that promotes competition and security in our nation's telecommunications technology. I also applaud the Energy and Commerce Committee for tackling an issue much larger than spectrum allocation alone, by examining the tough questions that will shape the future and role that small businesses play in innovation, connectivity, and America's future.

Sincerely,



Nicholas J. Pisciotta
Chief Executive Officer
Sicuro Innovaitons LLC
6302 Crosswoods Circle
Falls Church VA, 22044



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON DC

Mike O'Rielly
Commissioner

May 16, 2018

The Honorable Marsha Blackburn
Chairman
Subcommittee on Communications and
Technology
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Michael F. Doyle
Ranking Member
Subcommittee on Communications and
Technology
House Energy and Commerce Committee
2322A Rayburn House Office Building
Washington, DC 20515

Dear Chairman Blackburn and Ranking Member Doyle:

Thank you for convening this important hearing to examine telecommunications, global competitiveness, and national security. As I'm sure you know, the Federal Communications Commission (FCC or Commission) has also been focused on these issues, particularly the security of the telecommunications supply chain. As our recent Notice of Proposed Rulemaking on supply chain security proceeds forward, the Commission is appropriately considering the role and influence of Team Telecom in any pertinent future decisions. Therefore, I respectfully request that as Members consider ways to promote or investigate these issues, you include in your consideration potential reforms to the Team Telecom process as part of the jurisdictional referral of H.R. 4311, the Foreign Investment Risk Review and Modernization Act. Moreover, to the extent that this or similar legislation is under consideration for being added to the annual National Defense Authorization Act bill, I would humbly suggest that addressing Team Telecom should be contemplated as part of those discussions as well.

As you know, the Commission consults with Team Telecom (which typically consists of the Departments of Commerce, Justice, State, Homeland Security, Defense, the Federal Bureau of Investigations, and the United States Trade Representative) on U.S. national security interests when reviewing applicable license applications involving foreign ownership. However, the Team Telecom process, which is not codified, is unnecessarily opaque and uncertain, and in need of reform.

Specifically, applications referred to Team Telecom – unlike those that go through the CFIRUS process – can take significant time to complete. The lack of statutory structure prevents sufficient promptness by the respective agencies. Meanwhile, entities have no ability to determine which agency or agencies have concerns or how to locate a point of contact within these government organizations to help facilitate a resolution. When entities do hear from Team Telecom, they can be subjected to multiple requests for information, some of which are beyond the scope of the foreign ownership being reviewed. Ultimately, this process delays applications for years and dissuades U.S. companies from considering new opportunities. Further, it effects

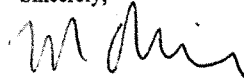
Page 2
May 16, 2018

the procedures used by foreign nations that govern the ability of U.S. companies to invest internationally.

There are several reforms to Team Telecom that, if implemented, I believe would greatly improve the process. These include: (1) setting and requiring Team Telecom to follow deadlines for recommendations to the Commission; (2) excluding pro-forma transfer and assignment applications and applications involving ownership structures previously reviewed favorably so that the burdensome Team Telecom review is not unnecessarily repeated when foreign ownership is not changed; (3) establishing standardized questions for necessary and relevant information collection by applicants; and (4) requiring each Executive Branch agency that submits views to the Commission to identify the individual point of contact within the agency.

I hope the Subcommittee will consider these proposed reforms to Team Telecom throughout its larger discussion of this timely topic. To help facilitate the Subcommittee's work, I am attaching draft language consistent with my recommendations outlined above. More importantly, I stand ready to work with this Committee on this important issue and thank Members for considering such a proposal.

Sincerely,

A handwritten signature in dark ink, appearing to read "M. Rielly", written in a cursive style.

Michael O'Rielly

Attachment

Sec. _____. Team Telecom Improvement.

- (a) Rulemaking -- Within 180 days after date of enactment, the Secretary of the Department of Commerce, in consultation with the Secretary of the Department of Homeland Security, Secretary of the Department of Defense, Secretary of the Department of State, U.S. Trade Representative, and the Attorney General (or their designees), shall issue final rules for the preparation and transmittal of Executive Branch views, as needed, on license applications and transfers involving foreign ownership pursuant to Section 310(b) of the Communications Act of 1934.
- (b) Content of Rules -- The rules issued pursuant to subsection (a) shall --
 - 1. Include deadlines, consistent with the review timelines contained in section 721 of the Defense Production Review Act of 1950 (as amended), by which such views are to be transmitted to the Federal Communications Commission;
 - 2. Exclude pro-forma transfer and assignment applications, applications solely pertaining to non-facilities-based resale authority, transfer and assignment applications where the ultimate owner was previously referred and received favorable views by the Executive Branch, applications in which the applicant certifies it has sought or will seek review and approval pursuant to section 721 of the Defense Production Review Act of 1950 (as amended); and others that would not require referral as determined by the Federal Communications Commission;
 - 3. Establish standardized questions for necessary and relevant information collection by any applicable applicants; and
 - 4. Require each Executive Branch agency that submits views to the Commission to identify the individual contact within that agency tasked with responsibility for such views.
- (c) Limitations on Authority -- Nothing in this section shall be interpreted as altering or expanding the authority of the Executive Branch over matters within the authority of the Federal Communications Commission or to interfere with the independence of the agency.

05

A U.S. Investment Strategy for Defense

Andrew P. Hunter

A key element in responding to China is to invest in the development of critical technologies in the United States. And while investing in research and development (R&D) is likely to be an obvious and relatively noncontroversial response, it is important to understand why and how this investment will pay off if we are to make the most of the resources dedicated to it. A strategy of investment worked for the United States in the last century and although the circumstances then were decidedly different, it remains relevant today. However, today's strategy must be tailored to reflect China's rise and to complement the increasingly commercial and global nature of R&D.

A Successful Defense Investment Strategy

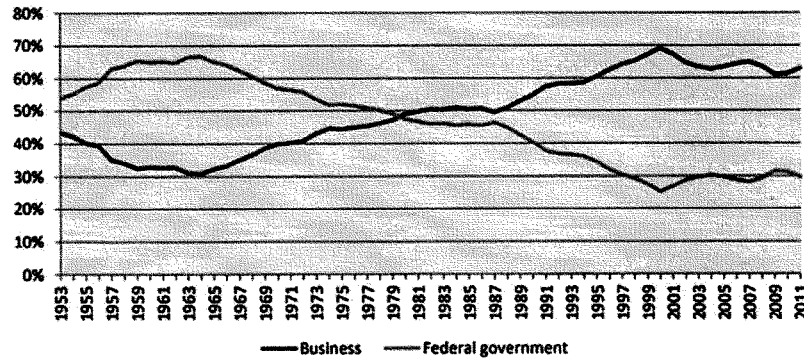
After World War II, the United States decided to make a massive investment in technology a key part of its strategy for global superpower competition. While the United States was not known for its investments in military technology prior to World War II, with the success of the Manhattan Project and the onset of the Cold War, the United States emphasized investing in technology as a linchpin of its strategy. Investment was central in the newly dawned nuclear age where it was believed that "strategic" systems, that is, nuclear weapons, would dominate the global security landscape. And while it became clear quickly that nuclear weapons were not going to end all nonnuclear competition, the United States remained committed to investing in technology to offset the numerical advantage in conventional forces that the Soviet Union and its allied Warsaw Pact countries had compared to the United States and its NATO allies.

The Department of Defense, along with NASA and the Atomic Energy Commission, invested heavily in R&D throughout the second half of the twentieth century resulting in the procurement of successive generations of technologically cutting-edge systems. The U.S. commitment to an investment strategy was so firm that in the mid-1960s, the U.S. government share of R&D investment represented two-thirds of total U.S. R&D, as shown in Figure 3. Total investment by the private sector was only a third of the U.S. total. A key feature of the U.S. investment strategy was scope and scale.

The Soviet Union was also investing in R&D throughout this period, and it had a cadre of talented researchers as well. The United States out-competed them, however, by ensuring that its investment in R&D was substantially larger, and by making investments across a huge range of technologies in a wide variety of fields. The Soviets proved unable to match, and increasingly fell farther behind. President Reagan's decision to invest heavily in missile defense in the 1980s is sometimes cited as a major reason the Soviet Union fell. In truth, the U.S. strategy of out-

investing the Soviet Union started much earlier and was much broader than this reading of history suggests. But the investment in missile defense does provide an illustration of the larger story of the success of the U.S. investment strategy. The U.S. investment strategy led to decades of technological superiority for U.S. military forces. It also had a wide variety of nonmilitary benefits, laying the foundation for technological advances such as GPS and the internet, which have delivered huge economic benefits.

Figure 3: Share of Funds for R&D in the United States, 1953–2011



Source: Ryan Crotty and Andrew Hunter, *Keeping the Technological Edge: Leveraging Outside Innovation to Sustain the Department of Defense's Technological Advantage* (Washington, DC: CSIS, June 2015), 9. Data derived from National Science Foundation, *Science and Engineering Indicators 2014*, National Center for Science and Engineering Statistics, National Patterns of R&D Resources (annual series).

The Changing Structure of Global R&D

A new U.S. investment strategy to compete with China can't simply be a copy of the approach taken in the second half of the twentieth century. The game has been fundamentally changed by the enormous increase in private-sector R&D, which completely reversed the ratio of government-to-private-sector R&D in the United States by the 1990s to favor the private sector. Equally important is the increasing globalization of R&D, driven in no small part by the rise of China, but also reflecting the R&D occurring in a variety of other nations. The dominance of private-sector funding for R&D means that key technologies such as artificial intelligence, robotics, additive manufacturing, space, and biotech will be fundamentally driven in most of the world by private-sector rather than government investment. The increasingly globalized nature of R&D means that most commercially driven technologies will be available to systems developers around the world. Most technologies are unlikely to remain the sole purview of any nation for more than a handful of years. These factors must lead the United States to develop a different investment strategy. There simply isn't much reason for the United States to use government resources to duplicate the work that the private sector will perform on its own.

Care must also be taken in developing military applications of commercial technologies that are also available to both allies and adversaries alike.

The Role for Government Investment

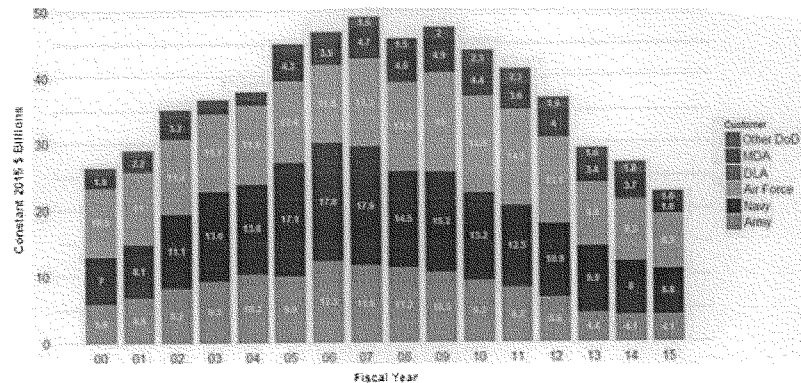
Government investment retains a critical role in a U.S. investment strategy, however, in making the kinds of investment that the private sector won't. The private sector primarily invests where it sees an attractive return on investment (ROI) in a time frame of five years or less. Only a relatively small number of companies have the resources and secure market position to make investments that need a decade or more to pay off. A related group of firms work in industries where the scope and scale of the work necessitates longer ROI time horizons, for example in designing and building large airframes or disrupting large entrenched industries, but even so they mostly focus on those investments with clear potential commercial ROI in the billions. Government investment must continue to fill the gap in funding early-stage R&D that hasn't yet demonstrated compelling commercial ROI.

Look deeply into the source of private sector R&D and you will usually find a history of defense research that pioneered the early stages of the technology. Frequently the Defense Advanced Research Projects Agency was a significant player in the early days of development of new technologies. Before the 1980s, NASA played a similar role for many space and aviation technologies though it has much reduced that role in recent decades. In addition to early-stage R&D, government investment is frequently necessary to apply cutting-edge commercial technologies to specific military problems. Commercial electronics may need to be adapted to operate in austere or extreme environments in military applications and additional features added. More extensive development may be required to convert commercially developed industrial capabilities to produce advanced military systems in the necessary performance regimes, such as fighter planes and the highly specialized engines that power them. In addition, government investment is often necessary to sustain the unique industrial capabilities that support these advanced military systems. The United States needs a strategy that supports these critical government roles.

A Defense Investment Strategy to Compete with China

The U.S. investment strategy that helped defeat the Soviet Union will not perform nearly as well if it is used as the strategy for competition with China. The changes in the structure of global R&D already discussed implicitly call into question the likelihood that a strategy of overwhelming scope and scale in R&D can be meaningfully executed. The growth of China's economy and the regime's clear commitment to R&D suggest, in fact, that the United States may soon be challenged to match the scope and scale of China's investment. While there will likely be a residual U.S. advantage in many military-related fields for several years, that advantage should be expected to erode without action. One clearly needed step is to recommit the United States to investment in defense R&D. The years since 2009 have seen an unprecedented decline in the defense R&D funding going to industry in constant dollar terms as shown in Figure 4.

Figure 4: DoD R&D Contract Obligations by Component, 2000–2015



Source: Jesse Ellman et al., *Defense Acquisition Trends, 2016: The End of the Contracting Drawdown* (Washington, DC: CSIS, March 2017), 19.

In fact, R&D is the only area of defense contract spending that did not increase in 2016, the year in which overall defense contract spending began to recover, and it is unlikely to recover significantly in 2017 or 2018. A concerted effort is needed to reverse this R&D contract decline and it must begin in earnest in the budget for fiscal year 2019. Other major sources of U.S. government R&D funding come from the National Institutes for Health, the Department of Energy, and NASA. While the R&D investment of these agencies didn't fall nearly as much as DoD's in the last several years, increasing their investment is also warranted. The key technology areas for investment are increasingly matters of consensus, and include the predominately commercial technology areas mentioned earlier as well as more military-specific technologies such as hypersonics, electronic warfare, energetic materials, and cyber-attack. The U.S. investment strategy should seek to complement and leverage the massive investments being made by the private sector (which typically builds on and exploits government-funded basic research) even as it focuses on the more military specific investments that the private sector is unlikely to pursue.

Invest in a More Flexible and Resilient Supply Chain

An increase in government-sponsored R&D as part of a U.S. investment strategy is necessary, but not sufficient, however. China is explicitly seeking to achieve market dominance in several key technologies, and China's past behavior suggests that it may seek this position in part to have the leverage to cut off access to critical resources to other countries. An example of this came in 2010 when China established strict export quotas on rare earth metals, effectively limiting access to nearly all of then-active world production to manufacturers in China. Rare earth metals are used in a wide variety of national security applications including missile guidance systems and power generation in addition to many important civilian applications. This

effort, if intended to force the on-shoring of upstream component production, largely failed because suppliers of rare earth metals elsewhere in the world were able to increase production as world prices of this resource increased. However, if China had been able to establish itself as the sole reliable provider of rare earth materials, it is very likely it could have leveraged that market power to establish dominance in making a series of critical components higher up the defense value chain.

The possibility that China will use whatever dominant market positions it achieves—and it will inevitably succeed in establishing significant market power in at least some technology areas as they have with solar photovoltaic panels—means that the U.S. investment strategy should focus, in part, on developing flexibility and resilience in the defense supply chain. China couldn't force rapid on-shoring of the production of components using rare earth metals in 2010, but it is not inconceivable that it could try again and succeed in the future. It is also entirely possible that China could achieve such an outcome over time by working with, rather than against, market forces. However, there are substitutes for rare earth metals in most applications as there are for many other materials and technologies that China may seek to dominate. The U.S. investment strategy should include research into developing and making practical alternatives in key areas of the supply chain where U.S. access could be threatened, enabling the United States to reconstitute supply chains more quickly. This suggests a commitment to developing second sources of key components and materials wherever U.S. access could be cut off.

Leverage Partnerships with Other Nations

The U.S. investment strategy must also leverage the increasingly global structure of R&D. In the twentieth century, the overwhelming scope and scale of U.S. investment in R&D was coupled with a strict technology control system designed to keep the fruits of all that investment in the United States, with some limited access also provided to allies on a case-by-case basis. But R&D today is already far more diffuse and egalitarian than it was during the Cold War. Many U.S. partners and allies are also making key R&D investments and cutting-edge technologies are increasingly being developed outside the United States. The U.S. investment strategy should capitalize on, leverage, and enable complementary investments by partners and allies. We can do so by coordinating with key partners and allies to research critical technologies together or in complementary fashion. We can also increase our utilization of foreign designs (but with production in most cases in the United States) especially in areas where the United States has under-invested in the last decade, such as advanced protection capabilities for ground vehicles. A U.S. investment strategy that leverages the enormous investments being made by our partners will be more powerful and successful than one that attempts to utilize U.S. resources alone. This approach requires that the United States continue to modernize its technology control system to enable more cooperation with allies and partners, and to actively seek partners in the key technologies of the future through defense trade. Working with our allies can also make the response to aggressive efforts by China (or Russia) to use market power much more effective.

Develop, Attract, and Retain the Best People

The last key element of the U.S. investment strategy is people. The United States must invest in science, technology, engineering, and mathematics (STEM) education for any U.S. investment

strategy to succeed, and must create a cultural environment conducive to the development and success of technical talent. The United States is in a high-stakes competition for technical talent with every other nation in the world. A key factor in the success of the U.S. investment strategy of the twentieth century was the influx of technical talent from Europe and Asia that resulted from the World Wars. The United States has been a favored destination for innovators and the scientifically minded for decades. Nothing can be more critical than that it remain so. Happily, the fostering of domestic technical talent and the ability to attract foreign talent are highly complementary. The same conditions tend to lead to success in both cases. People are perhaps the most vulnerable aspect of this proposed U.S. investment strategy because China has an abundance of technical talent to draw upon. If the United States neglects this element of the strategy, or adopts policies that discourage technical talent from developing or coming to the United States, the rest of the strategy will likely have no meaningful effect.

Recommendations

- Increase U.S. investment in defense R&D focusing on basic research, leveraging commercial R&D for military applications, pursuing design and development of critical military technologies, and developing greater resilience in the U.S. supply chain.
- Leverage the R&D of partners and allies by cooperating in R&D of critical technologies and by purchasing and domestically producing foreign designs where they are best in world.
- Establish a research environment that fosters the development of U.S. technical talent and that attracts the best technical minds from other countries to the United States.

06

Beijing's Cyber Governance System

Samm Sacks

China is in the midst of building perhaps the most extensive governance system for cyberspace and information and communications technology (ICT) of any country around the world. Recognizing that technology has advanced more quickly than the government's ability to control it, Beijing has moved to rapidly to construct a policy framework spanning cybersecurity, the digital economy, and online media content—all under one mantle.

A matrix of national strategies, laws, measures, regulations, and standards together make up China's vision to become a "cyber superpower" and build a robust ICT governance system. These elements are mutually reinforcing, and lay out requirements that cover data transfer, data privacy, critical information infrastructure, internet content, and ICT industrial development.

The build-out of China's ICT governance system has implications both for U.S. companies operating in China, as well as for Chinese investment flowing into the United States and globally. For U.S. companies, regulatory uncertainties and costs for operating in China are rising, compelling many to reassess the tradeoffs required to be in China. At the same time, there are major national security and trade implications for the global expansion of Chinese firms and capital in ICT sectors. As this system takes shape, understanding the overall framework as well as its individual elements will be key for U.S. policymakers. Some parts are final, but many are still pending as stakeholders within the Chinese bureaucracy continue to debate their scope and implementation.

Understanding China's emerging cyber regulatory system will be critical in order to craft a precise and targeted U.S. policy response as U.S.-China trade risks grow. Calibrating the right approach to the challenges posed by China must begin with an accurate view of this complex system, one that is often misunderstood by outside observers.

What Beijing Requires of ICT Companies in China

China's Cybersecurity Law (which took effect in June 2017) is the centerpiece of a much broader ICT regulatory system made up of dozens of interlocking parts. There are three main ICT regulatory concerns for foreign companies operating in China: "black box" cybersecurity reviews, restrictions on cross-border data transfer, and an overall trend toward localization under the guise of security.

ICT Security Reviews

Foreign companies now face at least six different security reviews that can be used for political purposes to delay or block market access. These reviews will be conducted by different Chinese government agencies with unclear jurisdictions. There is even conflicting jurisdiction within individual reviews. Moreover, the specific criteria, metrics, and, in some cases, those conducting the evaluations are not known. As several U.S. industry representatives put it, the reviews are essentially a “black box” because we do not know what they entail and what is required to pass them. Some have lobbied the Chinese government to accept international security certifications (such as through ISO) as a basis for compliance, but so far it is not clear if Chinese authorities will recognize these certifications or still require their own reviews.

Coming actions to expand the scope of the Committee on Foreign Investment in the United States (CFIUS) could lead Beijing to likewise use these security reviews as channels to retaliate against U.S. companies operating in China. Since there is no transparency into the process, these reviews can easily become political tools, with U.S. companies on the frontlines as bilateral tensions increase.

The different cybersecurity reviews, and their practical implications, are discussed below:

1. *The Multi-level Protection Scheme (MLPS)*: MLPS is managed by the Ministry of Public Security (MPS) and has existed since 2006. MLPS will likely undergo revisions as part of the new ICT legal regime, but coming changes, as well as how it will be coordinated with other similar security reviews, remain unknown. MLPS involves ranking networks by level of sensitivity, and then assigning certain compliance obligations.
2. *Cybersecurity Review Regime*: A key question is how MLPS will work in relation to a new review known as the Cybersecurity Review Regime (CRR) or Cybersecurity Review Measures of Network Products and Services. Issued in “interim” form in June, the measures require network products and services used in critical information infrastructure (CII) to undergo a cybersecurity review administered by the Cyberspace Administration of China (CAC) and other sector-specific regulators. Some industry experts believe that the CRR will involve inspections of the backgrounds and supply chains of network and service providers. The final definition of CII is still pending, and the full criteria for assessments and list of those conducting them are unknown. Yet, without these pieces of the puzzle, the practical implications of this system remain murky.

The government has begun to issue several other documents meant to provide more clarity on the scope of the new review regime. These include the “Public Announcement on Issuing Network Key Equipment and Cybersecurity Special Product List (First Batch),” which outlines a list of products and services subject to the review and certification. There are also at least three relevant standards that have not yet been officially published. Yet, the follow-on product list and standards do little to narrow the far-reaching scope of the CRR. That is because the “interim” document establishing the CRR states that the review will focus on “other risks that could harm national security”—essentially preserving government authority to interpret the scope of reviews however it

wants. Again, this is a channel that opens the door for political whim to determine market access.

3. *Reviews of Cross-border Data Transfer:* In addition, there will also be separate security review of data that companies seek to transfer outside of mainland China. The government is in the process of refining the process and conditions under which data would undergo a security assessment under two draft regulations: Personal Information and Important Data Cross Border Transfer Security Evaluation Measures and Guidelines for Data Cross-Border Transfer Security Assessment. Again, the specific scope is not yet clear, but according to industry sources inside China, it is likely that Chinese authorities will take a broad and ambiguous approach to enforcement of this particular review. (See following section on "Data Localization.")
4. *Cross-border Communications:* Although not a security review per se, companies operating in China must have authorization from the Ministry of Industry and Information Technology (MIIT) for using internal company VPN (virtual private network) services. In practical terms, this means that the government reviews and approves the channels that companies use for all of their international connectivity. Requirements issued by MIIT in 2017 mandate that companies only use internal VPN services from licensed providers, which are the three state-owned telecommunications carriers. Cloud service platforms must route communications with their overseas facilities through channels approved by MIIT.
5. *Internet Technologies and Apps:* New technologies and apps used in internet news/information services also have a new security review process. Service providers must conduct security evaluations before the introduction of new technologies or applications on their platforms, but details are also murky.
6. *A Possible Chinese Version of CFIUS:* Much less is known about another possible kind of security review of foreign investment that has yet to emerge. China's National Security Law (released in 2015) suggested in broad language there could be a new body perhaps akin to CFIUS. There has yet to been further clarification. New legislation expanding the scope of CFIUS could trigger Beijing to move forward setting up this new mechanism.

Data Localization

Many U.S. firms in China already assume that data localization requirements will become the de facto reality for their China operations. The specific scope of data localization requirements is still in flux; yet, some Chinese companies have even stopped sending their data to foreign companies that had the ability to store and process data within mainland China, despite there being no set requirement for them to do so.

There are provisions still in draft form that would require certain kinds of data to be stored within mainland China and require approvals for cross-border data transfer. Below are the relevant laws, measures, and standards on the issue:

According to article 37 of China's cybersecurity law: "Personal information and other important data gathered or produced by critical information infrastructure operators during operations within the mainland territory of the People's Republic of China, shall store it within mainland China." The government is still defining "personal information and other important data" or what sectors fall under "critical information infrastructure" under separate measures and guidelines, but early indications suggest even follow-on directives will be vast and ambiguous. This also underscores the fact that China's ICT legal framework is best understood as a matrix of overlapping parts. Recently, Chinese officials have been asking U.S. government and business leaders for advice on how to define critical information infrastructure, suggesting the parameters are still in flux and open to interpretation.

Following on the Cybersecurity Law, the Chinese government issued a measure and standard meant to clarify the scope of how restrictions on cross-border data transfers will be implemented. The problem is that these follow-on directives are equally vague and leave issues unresolved as different stakeholders within the Chinese system debate their meaning. First is the "Measures on Security Assessment of Cross-border Transfer of Personal Information & Important Data (Draft for comment)." Companies have until December 2018 to comply. Several internal versions of the draft have been quietly circulated in the past few months. According to the latest publicly available draft, all "network operators" will be subject to assessments before exporting data out of China. In practice, this could mean anyone who owns and operates an IT network. Industry sources report the government may have walked this back recently to focus just on CII operators, but there is still tremendous regulatory uncertainty given that the definition of CII itself is up in the air.

In addition, the National Information Security Standardization Committee (TC260)—China's cybersecurity standards body—issued a standard to flesh out technical guidelines assessing cross-border data transfers. Yet, the language even of this technical standard is extremely vague and far-reaching. The May 27 version gives a sweeping definition of "important data" that echoes the National Security Law, spanning that which can "influence or harm the government, state, military, economy, culture, society, technology, information . . . and other national security matters." Again, "network operators" could mean anyone who owns and manages an IT network, raising the possibility that e-commerce could be deemed CII given all the personal data held by companies like Alibaba and Tencent. Depending on how CII is ultimately defined, many companies that are not in ICT sectors could potentially fall in scope. Chinese regulators are now studying how countries like the United States define CII through numerous Track 1.5 dialogues. While regulators are showing a willingness to engage and dialogue, it is not clear how these exchanges will ultimately impact Beijing's policy trajectory, particularly since Beijing views this as primarily a national security rather than trade issue.

China vs. EU and APEC on data restrictions

These reviews are not comparable with requirements under international regimes such as the voluntary Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) or the EU's General Data Protection Regulation (GDPR). The EU views data protection primarily through the lens of user privacy. In contrast, passing one of the Chinese reviews for outbound data transfer is linked not merely to personal privacy or raw data security, but also to "national

security” and broader, more ambiguous concerns like “the people’s livelihood” (Cybersecurity Law Article 31) or “economic development and social and public interests,” according to the guidelines. Some industry groups are hoping that China might accept CBPR in place of their own data review system, but this looks unlikely given that China appears to want its own system.

Internal Debate within China over Data Flows

While China’s regulatory regime for data flows looks bleak, there are also competing voices in China advocating for more alignment with international practices. These voices should not be disregarded by U.S. policymakers. Key players in China think that cutting off cross-border data flows will hurt the country’s global economic goals. From national tech champions like Alibaba seeking global markets, to Chinese financial institutions facilitating global transactions, cross-border data flows are a core operational reality. These voices also exist within the Chinese government. For example, Hong Yanqing, who leads the personal data protection project for TC260, writes: “A fundamental consensus has emerged today that data naturally flows across national borders, that data flows produce value, and that data flows can lead to flows of technology, capital, and talent.” These players could be important allies for the United States.

Localization Push under “Secure and Controllable”

Foreign companies face de facto localization pressures in China even in the absence of specific regulation. The Xi Jinping administration has emphasized through multiple channels that it seeks to bolster China’s domestic ICT industry to reduce reliance on foreign core technologies. The most recent is a report by the National People’s Congress in December underscoring the need for China to develop “indigenous and controllable core cybersecurity technology by 2020.”

For several years, the government has used the phrase “secure and controllable” or “indigenous and controllable” in national strategies and directives as a way to link localization with security. Chinese companies have a competitive advantage when it comes to meeting these new security standards. This puts foreign ICT companies in a weaker negotiating position, and adds to pressure that they cooperate with local partners, rather than attempting to go it alone in the market.

The phrase has appeared in separate rules and strategies for cyberspace and the ICT industry. The phrase appears in sector-specific insurance, medical devices, and the Internet Plus sectors (i.e., smart technology, cloud computing, mobile technology, and e-commerce). A requirement for banking-sector IT to be “secure and controllable” was technically suspended, but many report that it still has negatively impacted market share. The phrase is also sprinkled throughout national-level blueprints for ICT development. For example, the 13th Five Year Plan for Informatization calls for “building a secure and controllable IT industry ecosystem.”

Because this standard has no single definition, the government and Chinese industry have broad discretionary authority to launch intrusive security audits or reject foreign suppliers altogether as not secure. And while many of these regulations are still pending, Chinese government and industry are already moving forward with informal implementation of the standard, by asking foreign vendors to certify that they are “secure and controllable.”

Beijing's Vision for Making China a Global ICT Superpower

What makes China's cyber governance system so vast is that it does not just cover cybersecurity, but also establishes a top-down plan for advancing China's domestic ICT industry. Multiple overlapping strategy and planning directives all stress the need for China to be a global leader in advanced ICT, with Chinese companies at the forefront. These are not just empty slogans, but supported by detailed policy blueprints laying out the government's goals to reduce reliance on foreign technology to boost self-sufficiency in key fields, while increasing the global influence of China's national tech giants.

The "Made in China 2025" has received the most attention outside of China, but when it comes to ICT sectors there are other, more detailed policy directives spelling out what Beijing hopes to achieve. Three recent examples, summarized below, stand out as especially clear articulations of Beijing's objectives (there are many more):

- During President Xi Jinping's opening speech at the 19th Party Congress in October 2017, he called for the "deep integration of the Internet, big data, and artificial intelligence with the real economy" and for building a "science and technology superpower, quality superpower, aerospace superpower, cyber superpower . . . advancing the development of big data, cloud computing, and smart cities so as to turn them into a digital silk road of the 21st century." The speech marked the first time that an opening speech identified specific terms such as artificial intelligence (AI) and "digital China," suggesting these sectors will be priorities for Xi's second term.
- China's 13th Five Year Plan for Informatization (2016–2020) states that China strives to "no longer [be] restrained by others for core technologies in strategically competitive fields," and identifies major projects slated for increased state support in "core electronic equipment, high-end universal chip, basic software, large-scale IC, next-gen wireless broadband mobile communication, quantum communication and quantum computing."
- Another example is language from an article published in September (just ahead of the 19th Party Congress) in a leading Party Journal by the Theoretical Studies Center Group under the Cyberspace Administration of China. The essay explains how to put into action President Xi's call for making China into a "cyber superpower." Among the many points in the essay, the authors write: "The global influence of Internet companies like Alibaba, Tencent, Baidu, Huawei, etc., is on the rise. . . . In 2016 on a global list of top 20 companies by market value, Chinese companies occupied seven slots."

Recommendations

China is certainly not closed to all U.S. ICT firms or those with a digital footprint in the market. But the costs required to operate in China are increasing, particularly in high-tech sectors. Issues include ICT infrastructure—from trouble using corporate VPNs to the need to build local data centers—and lack of transparency around new licensing and security certifications that can be used to delay or block market access. Taken together, these new regulatory risks are now leading companies to reassess the tradeoffs required to be in the market.

There are real national security and commercial risks to the United States posed by China's ICT policies. In this context, it is understandable that U.S. policymakers are seeking a more confrontational policy stance, using a package of actions beyond just high-tech sectors, including: coming announcements about the 301 investigation, CFIUS reform, and a broader Trump administration China strategy.

The problem is that without a targeted approach, U.S. businesses are likely to become collateral damage in a trade war between the United States and China that does not benefit either side. U.S. companies in high-tech sectors are likely to bear the brunt of the damage. Here is what is likely to play out in 2018 depending on how both sides manage coming risks to the relationship:

First, in anticipation of coming announcements on the 301 investigation, the Chinese government is already drawing up retaliation lists of U.S. companies in China. U.S. companies with viable domestic competitors in China will be particularly vulnerable to retaliation. In the ICT sector specifically, U.S. companies with domestic Chinese counterparts may see licenses canceled or denied under the umbrella of various cybersecurity reviews and certifications. The various cybersecurity reviews (discussed in section one) could become political channels for the government to delay or block market access in sectors where network products and services are subject to black box reviews.

Second, if backed into a corner, Beijing is not likely to engage further in exchanges that have become an important channel for sorting out implementation of cyber policies and laws. There are informal and Track 1.5 or Track 2 channels that could come to a halt, leading to more hardline positions on still-unresolved ICT regulatory issues. To be sure, some have found the Chinese side to be less responsive in these channels, but there are in fact notable exceptions.

For example, in April 2017 the Chinese government faced significant backlash from foreign and domestic industry when it released the first draft of measures that all "important data" remain inside mainland China. In response, and after extensive back and forth with industry, Chinese authorities revised the scope to only require that data from critical information infrastructure (CII) operators be stored locally. They also moved back the date for compliance. Since the definition of CII is still unresolved, the issue remains problematic, but it shows that Beijing is willing to take a more nuanced position under certain circumstances. There are other examples in which Chinese domestic industry have been important allies to U.S. companies on pending regulatory issues, despite being competitors. These local champions will become less helpful to U.S. partners as trade tensions spill over to affect the broader bilateral relationship.

Looking ahead in 2018, Beijing has a draft encryption law in the legislative process. If enacted and enforced, the law could require only pre-approved domestic encryption products—a red line for many foreign companies in China. There are numerous other examples in which the U.S. tech sector stands the most to lose in a possible trade war between the United States and China.

U.S. and Chinese technology development, supply chains, and commercial markets are tightly intertwined in such a way that a sweeping approach to China's ICT policies will hurt U.S. economic prosperity and our ability to maintain our edge in technology innovation. U.S. policymakers need to tailor their reviews of Chinese commercial investments and punitive

damages in a way that does not further hinder U.S. companies operating in an already difficult Chinese market. The best approach is one that takes a more nuanced view of the U.S.-China trade and investment relationship to mitigate these downside risks.

5/13/2018

In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser - WSJ

DOW JONES, A NEWS CORP COMPANY

Nikkei 22755.91 -0.01%

Hang Seng 31122.06 -1.02%

U.S. 10 Yr 1/32 Yield 2.965%

Crude Oil 70.68 -0.03%

Yen 109.28 -0.10%

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.wsj.com>.

<https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000>

BUSINESS

In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser

Some rural internet providers rely on telecom gear from China's Huawei, which faces potential new restrictions from FCC, Congress

By Drew FitzGerald and Stu Woo | Photographs by Michael Hanson for The Wall Street Journal

Updated March 27, 2018 2:40 p.m. ET

Here is a potential casualty of the U.S. government's escalating fight against Huawei Technologies Co.: rural phone companies and internet providers that depend on the Chinese giant's gear to connect their customers.

Large wireless providers including AT&T Inc. have long steered clear of Huawei, which has been effectively barred from big U.S. business since a 2012 congressional report alleged the Chinese government could force the company to exploit knowledge of how its equipment is designed to spy or launch cyberattacks—a charge Huawei has denied.

But many regional American providers of wireless, TV and internet services have flocked to Huawei, attracted by what they say are Huawei's cheaper prices, quality products and attentive customer service.

On Monday, the Federal Communications Commission proposed making it harder for these smaller carriers to pay for future purchases of telecom equipment from Huawei and Chinese peers. The rule would restrict companies from drawing on an \$8.5 billion government-run fund that, among other goals, helps connect rural America to the internet. The agency is now seeking public comment on the proposal.



Devon Mitchell and C.J. Christensen install a new cable in Hermiston, Ore.

Meanwhile, a congressional bill with some bipartisan support aims to prohibit carriers with any substantial amount of installed Chinese telecom equipment from federal-government contracts.

Huawei, the world's top maker of cellular-tower electronics and a major manufacturer of equipment for cable and internet providers, has been actively courting small-town internet

companies that wanted to replace old-fashioned landlines with high-speed internet connections—no small feat in a country where most rural residents are stuck with dial-up speeds.

The company flew some clients to the company's Shenzhen, China, headquarters, one stop on a nationwide tour that included visits to the Great Wall and ancient Terracotta Army, and delicacies including chocolate-covered duck liver.

<https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000>

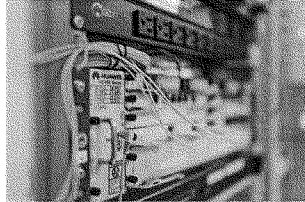
1/3

5/13/2018

In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser - WSJ

"They were hungry to break into the small market, and we like dealing with hungry vendors," said Jim Kail, chief of LHTC Broadband, a mostly rural internet provider in Pennsylvania with 7,000 customers. "They put a concentrated effort into it."

Mr. Kail's company in 2014 bought several hundred thousand dollars worth of optical network equipment—gear that can transmit data hundreds of times faster than a copper telephone line.



Eastern Oregon Telecom uses electronics made by Huawei.

Many of these customers now worry the new heat over Huawei in Washington may rob them of what has so far been an important alternative to Western suppliers. Others worry that if Huawei exits the U.S. completely, it will leave them without the customer and technical support they need to maintain the Huawei hardware they already own.

A Huawei spokesman declined to comment on the FCC proposal. He said the company is employee-owned and that no government has ever asked it to spy on or sabotage another country. Huawei said it poses no greater threat than its competitors, given they all share a global supply chain.

Huawei products make up less than 1% of the equipment in American cellular and landline networks today, according to research firm Dell'Oro Group. A senior FCC official said Monday that the government was concerned that it was "not zero."

Huawei's standoff with the U.S. government has been a boon to Sweden's Ericsson AB and Finland's Nokia Corp., which dominate the \$30-billion-a-year market for wireless equipment in the U.S. It also shields domestic companies like Silicon Valley's Cisco Systems Inc., which make electronics such as routers for cable and internet providers.

Joe Franell, the chief executive of Eastern Oregon Telecom, said his company added about 1,000 broadband customers after it took over unused cable lines that another provider had abandoned. He estimated that using new Huawei hardware on the previously offline system saved the company at least \$150,000.

"Our margins are pretty thin," Mr. Franell said. "If you start dictating what kind of equipment I can use, it tips the scales." He said he thinks the new legislation making the rounds in Washington is more likely driven by nationalism and protectionism than by real concerns about hacking and spying. "I'm not going to rework my whole business plan based off a rumor or an unsubstantiated allegation," he said.

Some politicians have raised more specific national-security issues related to Huawei gear in rural networks. Rep. Liz Cheney, the Wyoming Republican, was the original co-sponsor of a House bill to ban the U.S. government—or any of its contractors—from using equipment from Huawei or China's ZTE Corp. ~~ZTECOY-15.37%~~ The bill now has 43 co-sponsors, including four Democrats. Her big concern: Troops at U.S. military bases, which are sprinkled across parts of rural America that are often serviced by small carriers, could be at risk.

"We cannot allow the Chinese government to use entities like Huawei to gain access to our communications networks, including on our military bases," Ms. Cheney said in a statement.

It is unclear whether small carriers using Huawei equipment directly provide service to U.S. military bases. ZTE representatives didn't return requests for comment.

Write to Drew Fitzgerald at andrew.fitzgerald@wsj.com and Stu Woo at Stu.Woo@wsj.com

Appeared in the March 28, 2018, print edition as 'Rural Networks Feel Sting of Huawei Curbs.'

5/13/2018

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings - WSJ

DOW JONES, A NEWS CORP COMPANY

Nikkei **22756.74** -0.01% ▼Hang Seng **31122.06** 1.02% ▲U.S. 10 Yr **1/32 Yield** 2.965% ▲Crude Oil **70.69** -0.01% ▼Yen **109.29** -0.09% ▼

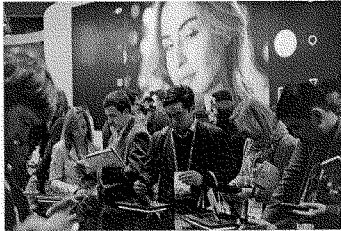
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<https://www.wsj.com/articles/huawei-long-seen-as-spy-threat-rolled-over-u-s-road-bumps-1515453829>

BUSINESS

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings

Chinese telecom giant has gobbled up huge global market share; now Washington is warning anew about alleged spy threat as U.S. telecoms embark on \$275 billion 5G network build-out



Huawei Technologies Co. showed off a new smartphone at last year's Mobile World Congress in Barcelona. PHOTO: JORDI BOIXAREU/ZUMA PRESS

By *Stu Woo, Dan Strumpf and Betsy Morris*

Updated Jan. 8, 2018 6:39 p.m. ET

SHENZHEN, China—Huawei Technologies Co. may be considered the bogeyman of the global telecom equipment industry in some Washington circles, but in Mountain View, Wyo., it's a hero.

That's where Union Wireless, a 103-year-old carrier that provides telephone and wireless service to 50,000 customers in five Western states, is singing its praises. Four years ago, Union turned to Huawei after its previous equipment vendor fell behind schedule on a critical network upgrade, says Brian Woody, customer relations chief.

Huawei "worries about getting the problem fixed first and then worries about getting paid," Mr. Woody says, which is important to a family-owned business working to maintain communication systems in mountainous territory. "We've had many vendors over the years. Huawei has treated us better than anybody."

Huawei appeared shut out of the U.S. six years ago after congressional investigators determined that its equipment could be used for spying or crippling the U.S. telecommunications network. Their conclusions and recommendations, delivered in a report in 2012 just as Huawei was gaining traction in the U.S., effectively killed Huawei's chances to win

<https://www.wsj.com/articles/huawei-long-seen-as-spy-threat-rolled-over-u-s-road-bumps-1515453829>

1/5

5/13/2018

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings - WSJ

business from major U.S. carriers. There was no law saying they couldn't partner with Huawei, but the political costs could have been steep.

Not so for small carriers such as Union Wireless, which fly under the national radar. The Chinese telecom giant has given them a much-needed equipment option in a quickly narrowing field. Four years ago, Mr. Woody says he had about five suppliers besides Huawei to choose from. Today, he has only two.

Now the U.S. telecom industry is in a bind. Huawei has positioned itself to dominate future global telecom networks, according to several U.S. telecom executives, providing stiffening competition to incumbents Nokia Corp. of Finland and Sweden's Ericsson AB. This comes just as big U.S. carriers are expected to invest about \$275 billion over seven years to deploy fifth generation, or 5G, networks that can carry huge amounts of data for high-quality mobile video and self-driving cars, according to Accenture. Early commercial deployments of the technology are to start later this year.

Since 2012, Huawei has expanded to 170 countries from 140, and now claims 45 of the world's 50 biggest wireless carriers as customers. Huawei, which also runs a popular smartphone brand, made \$75 billion overall in 2016. About \$26 billion came from its telecom equipment and software business, making it the leader in the \$126 billion-a-year global market, according to research-firm IHS Markit Ltd.

Huawei's dominance is again stoking fears among Washington security and intelligence experts, who worry major U.S. carriers might be tempted to turn to Huawei.

Last month, members of the Senate and House intelligence committees sent a letter asking the Federal Communications Commission to review any relationship with Huawei and requested that the FCC get briefed on the security concerns raised in 2012. The letter also raised concerns about Huawei's growing smartphone business, now the world's No. 3 brand behind Samsung Electronics Co. and Apple Inc.

The pressure may have already had an impact. Huawei planned to announce Tuesday at a Las Vegas trade show that it had struck an agreement to sell its smartphones through AT&T Inc. Instead, say people familiar with the matter, AT&T walked away from the deal. It couldn't be determined why AT&T, the country's No. 2 carrier by subscribers, changed its mind.

An AT&T spokesman declined to comment. A Huawei spokesman declined to comment on conversations with AT&T, saying only that "Huawei has proven itself by delivering premium devices with integrity globally and in the U.S. market." Though it can't sell smartphones bundled with service plans in Verizon or AT&T shops, Huawei makes them available to U.S. consumers online through Amazon.com and in stores at Best Buy.

All this frustrates Huawei. Ken Hu, one of Huawei's three chief executives, said in a recent interview the company isn't a security threat. Its "global business is testament to the fact that Huawei is not a vehicle for any government or any agency of putting surveillance on another country," he says.

Part of the suspicions about Huawei stem from its origins. It was founded in 1987 by Ren Zhengfei, a former engineer for China's communist People's Liberation Army. Huawei today has three CEOs, who take rotating turns at the helm. Mr. Ren, now 73, remains deputy chairman and de facto boss.

Mr. Ren started Huawei with \$3,200 when he was 43 as a telephone-switch resale business. The businessman shocked employees early on by telling them the company would one day be China's biggest telecom-equipment provider, recalls Richard Yu, now head of Huawei's consumer business. "Oh my God. Everybody was wondering whether we can survive."

5/13/2018

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings - WSJ



Ken Hu, one of three rotating CEOs of Huawei Technologies Co. PHOTO: TOMOHIRO OHSUMI/BLOOMBERG NEWS

It did.
After
succeed
ing in
rural
China,
Huawei
moved
into
places
that
Wester
n
compan

ies had overlooked or avoided—underdeveloped markets in Africa and Latin America.

RELATED

- AT&T Backs Off Deal to Sell Smartphones From Huawei
- China's Internet Giants Face Users' Anxiety Over Privacy

Eventually, to help Huawei expand globally, Mr. Ren learned Western business management practices, in part from International Business Machines Corp., which was trying to expand in China. IBM helped Huawei learn disciplines such as product development and financial

management. That and its improving technology helped Huawei gain ground in Europe, where its major customers today include Britain's Vodafone Group PLC, France's Orange SA and Germany's Deutsche Telekom AG.

European mobile operators also liked that Huawei offered a wider range of products than competitors and top-notch customer service, according to current and former European wireless executives.

Smaller U.S. carriers had similar experiences. When wireless upstart Clearwire chose Huawei as a major vendor in 2010, the Chinese firm assigned nearly 800 engineers to the project, a person familiar with the effort recalled. A problem discovered one day would be solved by the next, the person said, unlike some other vendors that would debate whose fault it was before fixing it.

When Sprint Corp. moved to acquire Clearwire in 2012, the year Congress issued its report, the U.S. government required that Huawei's equipment be removed from Clearwire's network. It eventually found replacements, but with regret.

"Their design cycles, their innovation cycles, I think have been the fastest of anyone I've seen because they have the R&D resources to throw at these things," this person said.

Early on, Huawei was notorious for reverse engineering competitors' products, most notably in 2003, when Cisco sued, accusing Huawei of copying router code down to identical model numbers to make it easier for Cisco customers to switch to less expensive Huawei versions. Huawei settled the suit without admitting wrongdoing and agreed to stop selling the routers.

Eventually, though, Huawei ramped up its own research and development, spending \$11.8 billion in 2016. Ericsson and Nokia, which lack Huawei's major consumer business, spent \$3.8 billion and \$5.9 billion, respectively.

Huawei began to compete against U.S. tech companies for talent, and built a campus in the bustling southern Chinese city of Shenzhen that looks as if it belongs in Silicon Valley. Employees come to work in T-shirts and sneakers.

<https://www.wsj.com/articles/huawei-long-seen-as-spy-threat-rolled-over-u-s-road-bumps-1515453829>

3/5

5/13/2018

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings - WSJ



Huawei founder Ren Zhengfei, right, shows Chinese President Xi Jinping around the company's London offices. PHOTO: MATTHEW LLOYD/BLOOMBERG NEWS

Union Wireless says it learned about Huawei by word-of-mouth from another small carrier. Huawei also sponsored the Rural Wireless Association's networking lounge at a big mobile-industry trade show in San Francisco last September.

Huawei engineers and executives also make regular visits to U.S. carriers to show off new technology, and the potential cost savings are "significant"—sometimes even half off competitors' prices, says one former U.S. telecom executive.

In August 2016, it looked like Huawei might get a seat at the table when AT&T published a list of possible 5G vendors that included not just Ericsson and Nokia but also Huawei.

In the following weeks, when congressional staffers met with AT&T executives in Washington to express concerns, they were told Huawei was offering equipment for 70% less than competitors, according to a person familiar with the meeting. AT&T executives told staffers they felt trapped between the security concerns and their duty to shareholders.

National Security Agency director Michael Rogers and James Comey, then-director of the Federal Bureau of Investigation, personally spoke to senior AT&T management, the person said.

AT&T declined to comment on the extent of its discussions with Huawei. "We expect to solicit information and bids from a large number of equipment providers as we continue to build out our next generation networks," an AT&T spokesman said.

Huawei disputed the characterization of its conversations with AT&T, saying it wouldn't have known how much its 5G equipment and services would cost in 2016 because it was well before international 5G standards had been set.



Huawei's Paris offices. PHOTO: LUDOVIC MARIN/AGENCE FRANCE PRESSE/GETTY IMAGES

An FBI spokeswoman and a lawyer for Mr. Comey declined to comment. The NSA didn't respond to requests for comment.

Recently, Huawei's Mr. Hu said it would be open to employing in the U.S. a model he says alleviated security concerns in Britain—a lab near

5/13/2018

Huawei, Seen as Possible Spy Threat, Boomed Despite U.S. Warnings - WSJ

Oxford, England, where employees with British security clearance physically disassemble Huawei equipment and inspect the hardware and software for vulnerabilities and "back doors." Huawei funds and operates the lab, which is overseen by a board with senior British intelligence and government officials, as well as one Huawei executive as the vice chair.

British authorities say the arrangement is working. In its most recent annual report, published in April 2017, the board concluded that the lab "fulfilled its obligations in respect of the provision of assurance that any risks to U.K. national security from Huawei's involvement in the U.K.'s critical networks have been sufficiently mitigated."

Nigel Inkster, a former director of operations and intelligence at MI6, the British foreign intelligence agency, isn't so sure. He says the lab was set up "to calm the concerns of the British government. It could be seen as closing the door after the horse has bolted."

It's a dilemma for the industry—and eventually consumers. Huawei's meager presence in the U.S. market is one of the reasons for the high cost of U.S. wireless service, says Stephane Teral, executive research director at IHS Markit.

U.S. wireless service costs \$41 per month per customer on average, according to the data and analytics firm—second only to Canada, which also largely discourages Huawei equipment. In the U.K., where Huawei is allowed but closely scrutinized, the average wireless bill is \$23 a month.

Meanwhile, the field of competitors has dwindled. French-based Alcatel and U.S.-based Lucent merged in 2006, and Nokia ended up buying the combined Alcatel-Lucent company in 2016. Nortel Networks Corp. folded in 2009 in Canada's biggest bankruptcy case.

Both Nokia and Ericsson have warned that 2018 will be challenging. Ericsson has changed chief executives, laid off thousands of employees, warned of sales cancellations and faces pressure from an activist investor. Ericsson and Nokia's combined revenue is less than that of Huawei.

U.S. security officials and telecom executives alike worry about an increasingly lopsided landscape. Says Mike Rogers, the former congressman who chaired the House intelligence committee and co-wrote the 2012 report on Huawei: "Given current market trends, it's hard to imagine Huawei not being the only option in 10 years."

—Ryan Knutson, Drew FitzGerald and Aruna Viswanatha contributed to this article.

Write to Stu Woo at Stu.Woo@wsj.com, Dan Strumpf at daniel.strumpf@wsj.com and Betsy Morris at betsy.morris@wsj.com

Appeared in the January 9, 2018, print edition as 'Huawei, Seen as Possible Spy, Boomed Despite U.S. Warnings.'

Copyright © 2017 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

UNITED STATES DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY
WASHINGTON, D.C. 20230

In the Matter of:

Zhongxing Telecommunications Equipment
Corporation
ZTE Plaza, Keji Road South
Hi-Tech Industrial Park
Nanshan District, Shenzhen
China

ZTE Kangxun Telecommunications Ltd.
2/3 Floor, Suite A, Zte Communication Mansion
Keji (S) Road
Hi-New Shenzhen, 518057
China

Respondent

ORDER ACTIVATING SUSPENDED DENIAL ORDER RELATING TO
ZHONGXING TELECOMMUNICATIONS EQUIPMENT CORPORATION AND
ZTE KANGXUN TELECOMMUNICATIONS LTD.

Background

On March 23, 2017, I signed an Order approving the terms of the Settlement Agreement entered into in early March 2017, between the Bureau of Industry and Security, U.S. Department of Commerce ("BIS") and Zhongxing Telecommunications Equipment Corporation, of Shenzhen, China ("ZTE Corporation") and ZTE Kangxun Telecommunications Ltd. of Hi-New Shenzhen, China ("ZTE Kangxun") (collectively, "ZTE"), hereinafter the "March 23, 2017 Order." Under the terms of the settlement, ZTE agreed to a record-high combined civil and criminal penalty of \$1.19 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

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 2 of 14

equipment to North Korea in violation of the Export Administration Regulations (15 C.F.R. Parts 730-774 (2017)) ("EAR" or the "Regulations"). ZTE also admitted to engaging in an elaborate scheme to hide the unlicensed transactions from the U.S. Government, by deleting, destroying, removing, or sanitizing materials and information.

Under the terms of the Settlement Agreement and the March 23, 2017 Order, BIS imposed against ZTE a civil penalty totaling \$661,000,000, with \$300,000,000 of that amount suspended for a probationary period of seven years from the date of the Order.¹ This suspension was subject to several probationary conditions stated in the Settlement Agreement and March 23, 2017 Order, including that ZTE commit no other violation of the Export Administration Act of 1979, as amended (50 U.S.C. §§ 4601-4623 (Supp. III 2015)), the Regulations, or the March 23, 2017 Order. The March 23, 2017 Order also imposed, as agreed to by ZTE, a seven-year denial of ZTE's export privileges under the EAR that was suspended subject to the same probationary conditions. The March 23, 2017 Order, like the Settlement Agreement, provided that should ZTE fail to comply with any of the probationary conditions, the \$300 million suspended portion of the civil penalty could immediately become due and owing in full, as well as that BIS could modify or revoke the suspension of the denial order and activate a denial order of up to seven years.

The Settlement Agreement and March 23, 2017 Order require that during the probationary period, ZTE is to, among other things, complete and submit six audit reports

¹ In addition to the BIS-ZTE settlement, ZTE Corporation entered into a plea agreement with the Justice Department's National Security Division and the U.S. Attorney's Office for the Northern District of Texas, and entered into a settlement agreement with the Treasury Department's Office of Foreign Assets Control. The civil penalties (including the \$661 million civil penalty imposed by BIS) and the criminal fine and forfeiture totaled, when combined, approximately \$1.19 billion.

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 3 of 14

regarding ZTE's compliance with U.S. export control laws. The Settlement Agreement and March 23, 2017 Order also include a broad cooperation provision during the period of the suspended denial order. This cooperation provision specifically requires that ZTE make truthful disclosures of any requested factual information. The Settlement Agreement and March 23, 2017 Order thus, by their terms, essentially incorporate the prohibition set forth in Section 764.2(g) of the EAR against making any false or misleading representation or statement to BIS during, inter alia, the course of an investigation or other action subject to the EAR.

On February 2, 2018, acting pursuant to the Settlement Agreement and March 23, 2017 Order, BIS requested, among other things, that ZTE provide a status report on all individuals named or otherwise identified in two letters sent by ZTE, through its outside counsel, to the U.S. Government, dated November 30, 2016, and July 20, 2017, respectively. The status report was to include, among other things, current title, position, responsibilities, and pay and bonus information from March 7, 2017 to the present. The first of those two letters, dated November 30, 2016, was sent during BIS's investigation of the violations alleged in the Proposed Charging Letter and referenced in the Settlement Agreement and March 23, 2017 Order. In that letter, ZTE described "self-initiated" employee disciplinary actions it asserted that it had taken to date and additional actions that the company said it would take in the near future because they were "necessary to achieve the Company's goals of disciplining those involved and sending a strong message to ZTE employees about the Company's commitment to compliance." The letter focused on ZTE's asserted commitment to compliance, including from the highest levels of management.

The July 20, 2017 letter, sent on ZTE's behalf during the March 23, 2017 Order's seven-year probationary period, also asserted ZTE's commitment to compliance and

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 4 of 14

claimed that the disciplinary actions taken had sent a very strong message to ZTE employees. The letter was sent “to confirm that the measures detailed by ZTE with respect to discipline have been implemented” against nine named ZTE employees identified during the U.S. Government’s investigation. The employee disciplinary actions—actions that ZTE told the U.S. Government that it had already taken—were in ZTE’s words a showing of ZTE’s “overall approach to discipline and commitment to compliance,” which the company described as “significant and sufficient to prevent past misconduct from occurring again at ZTE.” Nearly all of the employees named in the July 20, 2017 letter had been specifically identified to ZTE by the U.S. Government as individuals that U.S. law enforcement agents wanted to interview during the investigation, either because they were signatories on an internal ZTE memorandum discussing how to evade U.S. export controls, were identified on that memorandum as a “project core member” of that evasion scheme, and/or had met with ZTE’s then-CEO to discuss means to continue evading U.S. law. Three were members of the “Contract Data Induction Team” involved in extensive efforts to destroy and conceal evidence described in more detail below and in the PCL.

In sum, through those two letters, ZTE informed the U.S. Government that the company had taken or would take action against 39 employees and officials that ZTE identified as having a role in the violations that led to the criminal plea agreement and the settlement agreements with BIS and the U.S. Department of the Treasury’s Office of Foreign Assets Control. In fact, and as ZTE now admits, the letters of reprimand described in the November 30, 2016 letter were never issued until approximately a month after BIS’s February 2, 2018 request for information, and all but one of the pertinent individuals identified in the November 30, 2016 or July 20, 2017 letters received his or

her 2016 bonus.² These false statements were not corrected by ZTE even in part until March 2018, more than 15 months from ZTE's November 30, 2016 letter, approximately a year from the Settlement Agreement (which ZTE executed on March 2, 2017) and the March 23, 2017 Order, and nearly eight months from the July 20, 2017 letter. During a conference call on March 6, 2018, ZTE indicated, via outside counsel, that it had made false statements in the November 30, 2016 and the July 20, 2017 letters. As discussed below, ZTE's first detailed notification occurred on March 16, 2018.

Proposed Activation of Suspended Sanctions and ZTE's Response

On March 13, 2018, pursuant to Section 766.17(c) of the Regulations, BIS notified ZTE of a proposed activation of the sanctions conditionally-suspended under the Settlement Agreement and the March 23, 2017 Order, based on ZTE's false statements in its letters dated November 30, 2016 and July 20, 2017, respectively. The notice letter to ZTE also gave the company an opportunity to respond, which it did on March 16, 2018.

I have reviewed in detail ZTE's response. In its letter, ZTE confirmed the false statements and, as discussed further *infra*, posed certain questions in rhetorical fashion. ZTE then proceeded to summarize its response upon "discovering" the failure to implement the stated employee disciplinary actions prior to March 2018, including its decision to notify BIS of the failures. The company also described the asserted remedial steps it had taken to date, including the issuance in March 2018, of the letters of

² Some of the disciplinary actions ZTE discussed in its November 30, 2016 letter relate to employees who resigned from ZTE well before the date of that letter, including some even as far back as 2012 and 2013. ZTE asserted that such employees left the company by "mutual understanding." Including these employees allowed ZTE to inflate the number of employees listed as subject to disciplinary action, and the material provided by ZTE to date does not establish that they were, in fact, subject to such action. The false statements discussed as violations in this order do not include, however, ZTE's statements relating to the circumstances under which these employees left the company. Nor do the false statements at issue relate to an employee referenced in the July 20, 2017 letter, concerning whom ZTE did not clearly state that disciplinary action had been taken. This order also does not relate to any issues relating to the termination of four officials addressed as part of the criminal plea agreement.

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 6 of 14

reprimand that were to have been sent in 2016-2017. ZTE additionally asserted that, for current employees whose 2016 bonus should have been reduced (by 30% to 50%), it would deduct the corresponding amount from their 2017 annual bonuses "to the extent permitted under Chinese law." ZTE also said it will pursue recovery from (certain) former employees of bonus payments for 2016 that the company had informed the U.S. Government would be reduced, but, contrary to those statements, were paid in full. Finally, ZTE reiterated what it described as the company's serious commitment to export control compliance and summarized its plan to continue its internal investigation of the matter.

ZTE's Pattern of Deception, False Statements, and Repeated Violations of U.S. Law

In issuing the March 13, 2018 notice letter to ZTE, and in considering ZTE's response, I have taken into account the course of ZTE's dealings with the U.S. Government during BIS's multi-year investigation, which demonstrate a pattern of deception, false statements, and repeated violations. I note the multiple false and misleading statements made to the U.S. Government during its investigation of ZTE's violations of the Regulations, and the behavior and actions of ZTE since then. ZTE's July 20, 2017 letter is brimming with false statements in violation of § 764.2(g) of the Regulations, and is the latest in a pattern of the company making untruthful statements to the U.S. Government and only admitting to its culpability when compelled by circumstances to do so. That pattern can be seen in the November 30, 2016 letter, which falsely documented steps the company said it was taking and had taken, as well as in the 96 admitted evasion violations described in the PCL, which detailed the company's efforts to destroy evidence of its continued export control violations.

In agreeing to the Settlement Agreement and the imposition of the March 23, 2017 Order, ZTE admitted committing 380 violations of the Regulations as those

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 7 of 14

violations were alleged in BIS's PCL. The PCL detailed an extensive conspiracy, including as laid out in a 2011 company memorandum drafted by ZTE Corporation's Legal Department and ratified by its then-CEO, to evade U.S. export control laws and facilitate unlicensed exports to Iran. During the conspiracy, ZTE leadership and staff employed multiple strategies in an attempt to conceal or obscure the true nature and extent of the company's role in the transactions and thereby facilitate its evasion of U.S. export controls, of which ZTE had detailed knowledge. As a result of the conspiracy, ZTE was able to obtain hundreds of millions of dollars in contracts with and sales from Iranian entities to ship routers, microprocessors, and servers controlled under the Regulations for national security, encryption, regional security, and/or anti-terrorism reasons to Iran.

ZTE Cover-Up Activity

Of the 380 alleged and admitted violations, ZTE committed 96 evasion violations relating to its actions to obstruct and delay the U.S. Government's investigation.³ These violations included making knowingly false and misleading representations and statements to BIS special agents and other federal law enforcement agents and agency official during a series of meetings between August 26, 2014, and at least January 8, 2016, including that the company had previously stopped shipments to Iran as of March 2012, and that it was no longer violating U.S. export control laws. In doing so, ZTE acted through outside counsel, who were unaware that the representations and statements that ZTE had given to counsel for communication to the U.S. Government were false and

³ These 96 admitted violations are discussed in fuller detail in the Proposed Charging Letter attached to and incorporated by reference in the Settlement Agreement. In the Settlement Agreement, ZTE admitted each of the allegations and violations contained in the Proposed Charging Letter.

misleading. ZTE failed to correct those representations and statements, which were continuing in effect, until beginning to do so (via outside counsel) on April 6, 2016.

ZTE also engaged in an elaborate scheme to prevent disclosure to the U.S. Government, and, in fact, to affirmatively mislead the Government, by deleting and concealing documents and information from the outside counsel and forensic accounting firm that ZTE had retained with regard to the investigation. Between January and March 2016, ZTE went so far as to form and operate a "Contract Data Induction Team" made up of ZTE employees tasked with destroying, removing, and sanitizing all materials concerning transactions or other activities relating to ZTE's Iran business that post-dated March 2012. ZTE required each of the team members to sign a non-disclosure agreement covering the ZTE transactions and activities the team was directed to hide from the U.S. Government, subject to a penalty of 1 million RMB (or approximately \$150,000) payable to ZTE if it determined that a disclosure occurred.

Determination to Activate the Suspended Denial Order

It was with this backdrop in mind, as more fully alleged in the PCL, that the Settlement Agreement and the March 23, 2017 Order mandate that ZTE truthfully disclose, upon request, all factual information (not subject to certain privileges, which are inapplicable here), and that led BIS to make its February 2, 2018 request for information relating to the employee disciplinary actions stated in the November 30, 2016 and July 20, 2017 letters.

BIS has determined that the company's admission, in response to inquiries from BIS, that it made false statements to the U.S. Government during the probationary period under the Settlement Agreement and March 23, 2017 Order indicate that ZTE still cannot

be relied upon to make truthful statements, even in the course of dealings with U.S. law enforcement agencies, and even with the prospect of the imposition of a \$300 million penalty and/or a seven-year denial order. 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. BIS is left to conclude that if the \$892 million monetary penalty paid pursuant to the March 23, 2017 Order, criminal plea agreement, and settlement agreement with the Department of the Treasury did not induce ZTE to ensure it was engaging with the U.S. Government truthfully, an additional monetary penalty of up to roughly a third that amount (\$300 million) is unlikely to lead to the company's reform.

The false statements ZTE made in the July 20, 2017 letter violate Section 764.2(g) of the Regulations and the terms of the Settlement Agreement and the March 23, 2017 Order, and thus violate the conditions of ZTE's probation under the Agreement and the Order. The false statements in the November 30, 2016 letter, made during the investigation, are pertinent and material in at least two ways.⁴ First, they are evidence that ZTE's false statements to the U.S. Government did not cease in April 2016, as are the additional false statements ZTE made in its July 20, 2017 letter. Second, under Section 764.2(g) of the Regulations, all representations, statements, and certifications to BIS or any other relevant agency made, inter alia, in the course of an investigation or

⁴ They are also possibly material in another way, as the pertinent 2016 bonus payments may not have been made until after the Settlement Agreement had been executed or after it had been approved via the March 23, 2017 Order. The November 30, 2016 letter indicated that 2016 bonus figures would be "announced in March 2017."

ZTE Corporation and ZTE Kangxun
 Order Activating Denial Order
 Page 10 of 14

other action subject to the Regulations are deemed to be continuing in effect.

Notification must be provided to BIS and any other relevant agency, in writing, of any change of any material fact or stated intention previously represented, stated, or certified. Such written notification is to be provided “immediately upon receipt of any information that would lead a reasonably prudent person to know that a change of material fact or intention has occurred or may occur in the future.” 15 C.F.R. § 764.2(g)(2) (2014-2017).⁵ Thus, with regard to the probationary conditions at issue here, ZTE failed to comply even partially with this continuing duty to correct by written notification, from the date of the March 23, 2017 Order until March 8, 2018.⁶

I note that in its response to BIS’s notice of proposed activation of suspended sanctions and in making its case for leniency, ZTE acknowledged that it had submitted false statements, but argued that it would have been irrational for ZTE to knowingly or intentionally mislead the U.S. Government in light of the seriousness of the suspended sanctions. The heart of its argument is the question, posed by the company in rhetorical fashion, asking “why would ZTEC risk paying another \$300 million suspended fine and placement on the denied parties list, which would effectively destroy the Company, to avoid sending out employee letters of reprimand and deducting portions of employee bonuses?” ZTE argued that BIS should not act until the company completed an internal investigation so that ZTE could answer such questions.

⁵ Under the Regulations, “[k]nowledge of a circumstance (the term may be a variant, such as ‘know,’ ‘reason to know,’ or ‘reason to believe’) includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person’s willful avoidance of facts.” See 15 C.F.R. § 772.1 (parenthetical in original).

⁶ As discussed *supra* and in the March 13, 2018 notice letter, ZTE did provide some notice by telephone on March 6, 2018.

ZTE has posed such questions not because additional investigation could render its false statements true, but in the hope of postponing action by the U.S. Government and ultimately avoiding or minimizing the consequences of its additional violations. Similarly, additional time to continue its investigation is unnecessary and irrelevant to the issue of whether the company violated the provision against giving false statements to BIS under Section 764.2(g) of the Regulations, and in violation of the Settlement Agreement and March 23, 2017 Order. The reasons that ZTE violated the EAR are red herrings to BIS's concern that the company has repeatedly made false statements to the U.S. Government—as the company has now repeatedly admitted. As recently as March 21, 2018, in a certification to the U.S. Government signed by ZTE Corporation's Senior Vice President, Chief Legal Officer and Acting Chief Compliance Officer, ZTE admitted that it "had not executed in full certain employee disciplinary measures that it had previously described in a letter to the U.S. government dated November 30, 2016, and there are inaccuracies in certain statements in the letter dated July 20, 2017." Giving ZTE additional time to complete its internal investigation will not erase the company's most recent—in a series—of false statements to the U.S. Government.

Furthermore, ZTE's suggestion that it could or would not have made such a poor or irrational cost-benefit calculation, or otherwise assumed the risks involved, simply ignores the fact that throughout the U.S. Government's investigation ZTE has acted in ways that BIS would consider illogical and unwise. ZTE committed repeated violations of the Regulations and U.S. export control laws *while knowing and accepting* the most significant of liability risks, both before and after it knew it was under investigation. ZTE then raised the risks and stakes even further *while under investigation* by repeatedly lying to BIS and other U.S. law enforcement agencies and engaging in a cover-up scheme to destroy, remove, or sanitize evidence. The bottom line is that the proffered

ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 12 of 14

irrationality of the unlawful conduct does not excuse or minimize it; nor does the conduct stand alone, being part of an unacceptable pattern of false and misleading statements and related actions, as discussed above. Moreover, until BIS asked for all of the underlying documentation of the steps that ZTE said it had already taken, some of the most culpable employees faced no consequences—ZTE paid their bonuses and paid them in full and the employees went without reprimand. This is the message ZTE sent from the top.

Based on the totality of circumstances here, I have determined within my discretion that it is appropriate to activate the suspended denial order in full and to suspend the export privileges of ZTE for a period of seven years, until March 13, 2025.⁷

IT IS THEREFORE ORDERED:

FIRST, from the date of this Order until March 13, 2025, ZTE Corporation, with a last known address of ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan District, Shenzhen, China, and ZTE Kangxun, with a last known address of 2/3 Floor, Suite A, Zte Communication Mansion, Keji (S) Road, Hi-New Shenzhen, 518057 China, and when acting for or on their behalf, their successors, assigns, directors, officers, employees, representatives, or agents (hereinafter each a "Denied Person"), may not, directly or indirectly, participate in any way in any transaction involving any commodity, software or technology (hereinafter collectively referred to as "item") exported or to be exported from the United States that is subject to the Regulations, or in any other activity subject to the Regulations, including, but not limited to:

- A. Applying for, obtaining, or using any license, license exception, or export control document;

⁷ This date is seven years from the date of BIS's March 13, 2018 Notice of Proposed Activation of Suspended Sanctions and Opportunity to Respond in this matter.

- B. Carrying on negotiations concerning, or ordering, buying, receiving, using, selling, delivering, storing, disposing of, forwarding, transporting, financing, or otherwise servicing in any way, any transaction involving any item exported or to be exported from the United States that is subject to the Regulations, or engaging in any other activity subject to the Regulations; or
- C. Benefitting in any way from any transaction involving any item exported or to be exported from the United States that is subject to the Regulations, or from any other activity subject to the Regulations.

SECOND, no person may, directly or indirectly, do any of the following:

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

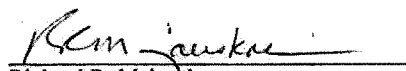
ZTE Corporation and ZTE Kangxun
Order Activating Denial Order
Page 14 of 14

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

THIRD, after notice and opportunity for comment as provided in Section 766.23 of the Regulations, any person, firm, corporation, or business organization related to a Denied Person by affiliation, ownership, control, or position of responsibility in the conduct of trade or related services may also be made subject to the provisions of this Order.

FOURTH, that this Order shall be served on ZTE, and shall be published in the *Federal Register*.

This Order is effective immediately.


Richard R. Majauskas
Acting Assistant Secretary of Commerce
for Export Enforcement

Issued this 15th day of April 2018.



US Army base removes Chinese made surveillance cameras

BY MAX GREENWOOD - 01/12/18 10:59 AM CST

44 SHARES

SHARE

TWITTER

7%

Just In...

GOP sen: Possible deal with ZTE 'a bargaining chip for Trump'
FINANCE — 3M 85 AGO

Senate Judiciary releases transcripts from Trump Tower meeting interviews
NATIONAL SECURITY — 10M 16S AGO

Sanders: White House 'leakers' should be fired
ADMINISTRATION — 15M 22S AGO

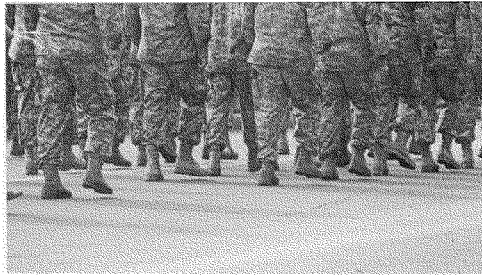
Senator weighs in on viral audio debate: 'I hear Laurel'
IN THE KNOW — 16M 57S AGO

Bill Gates spent \$44M to reform state education: report
NEWS — 16M 19S AGO

Art of the Deal co-author on McCain drama: Trump views apologizing as weakness
BLOG BRIEFING ROOM — 19M 48S AGO

Trump congratulates 'special guy' Barletta on win in Pennsylvania
BLOG BRIEFING ROOM — 43M 27S AGO

Following US lead, Guatemala moves embassy to Jerusalem



© Getty

The U.S. Army has removed security cameras manufactured by a company largely owned by the Chinese government from a military base in Missouri, [The Wall Street Journal reported](#) Friday.

The move came after The Journal reported on the prevalence of devices made by Hikvision. The Chinese government owns 42 percent of the company, which is the world's largest manufacturer of security cameras.

Col. Christopher Beck, the chief of staff at Fort Leonard Wood, told The Journal the Army never believed the cameras were a security risk, but decided to remove them to "remove any negative perception" surrounding the products.

Beck said the Hikvision cameras that were removed were not used to surveil high-security areas but were used to view roads and parking lots.

Hikvision has insisted its devices are secure, and the company has not been accused of using its devices to spy on behalf of the Chinese government.

A spokeswoman for Hikvision told The Journal the company "believes the products it builds and distributes around the world must meet the highest standards of not only quality but also security. We stand by our products and processes."

5/16/2018

BLOG BRIEFING ROOM
— 49M 46S AGO
[VIEW ALL](#)

US Army base removes Chinese-made surveillance cameras | TheHill

The company has also said it does not have access to cameras that have been sold to customers and the government-owned shareholder is not involved in Hikvision's day-to-day operations.

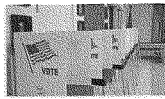
TAGS [HIKVISION](#) [FOR LEONARD WOOD](#) [SURVEILLANCE](#)

[SHARE](#)

[TWEET](#)

[PLUS ONE](#)

Related News by



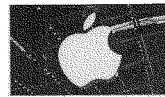
Homeland Security
sends officials to...



Ana Navarro: "White
House is irritated John...



Facebook reports spike
in violent content



Apple cancels \$1 billion
Ireland project over...



THE HILL 1635 K STREET, NW SUITE 900 WASHINGTON DC 20006 | 202-628-8500 TEL | 202-628-8503 FAX
THE CONTENTS OF THIS SITE ARE ©2018 CAPITOL HILL PUBLISHING CORP., A SUBSIDIARY OF NEWS COMMUNICATIONS, INC.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 1, 2018

Dr. Charles Clancy
Director and Professor
Hume Center for National Security and Technology
Virginia Tech
900 North Glebe Road
Arlington, VA 22203

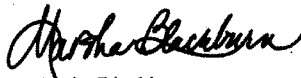
Dear Dr. Clancy:

Thank you for appearing before the Subcommittee on Communications and Technology on Wednesday, May 16, 2018, to testify at the hearing entitled "Telecommunications, Global Competitiveness, and National Security."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, June 15, 2018. Your responses should be mailed to Evan Viau, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed to Evan.Viau@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

cc: The Honorable Michael F. Doyle, Ranking Member, Subcommittee on Communications and Technology

Attachment

Responses to *Questions for the Record*

Dr. Charles Clancy, Professor of Electrical and Computer Engineering, Virginia Tech
before the House Energy and Commerce Committee, Subcommittee on Communications and
Technology, Hearing on Telecommunications, Global Competitiveness, and National Security

June 15, 2018

The following document provides responses to the questions for the record for the hearing entitled "Telecommunications, Global Competitiveness, and National Security" on May 16, 2018.

The Honorable Pete Olson

1. Some might say that the U.S. is already "catching up" with other nations in the race to 5G. Whether or not that is an accurate assessment, there are many more nascent technologies that are still in the early stages of development, such as AI, autonomous vehicles, robotics, and bio-tech to name a few. How do we ensure the US remains a competitive force in these fields while also guarding against national security threats?

The US Government spends \$140B per year on research and development (R&D), which is around 30% of total R&D investment in the US. These investments are crucial to helping the US remain competitive in the global innovation marketplace. While the US's R&D investment is increasing an average of 4.4% per year, China's investment is increasing at a rate of 16% per year, and is expected to overtake the US by 2020. Additionally in areas like bio-tech, China places fewer regulatory and ethical restrictions on research which affords them some unique advantages.

The US cannot out-spend China in R&D over the long term. Thus the US needs to be selective. Programs are needed to focus investments in areas critical to national security, such as those mentioned (AI, autonomy, bio-tech). Ordinarily this focused investment strategy would be overseen by the Office of Science and Technology Policy (OSTP) in concert with the major R&D investment departments and agencies; however, the lack of senior-level appointees and staff detailees makes it difficult for OSTP effectively execute this mission.

Recent White House coordination around Artificial Intelligence is a positive step forward. Similar efforts are needed in autonomy, quantum, and bio-tech. In all these areas a national strategy is needed that can help connect basic research funded by the National Science Foundation (NSF) and National Institutes

of Health (NIH) to the applied research envisioned by the Department of Defense (DOD) and Intelligence Community (IC) to tackle key areas of national security.

The Honorable Bill Johnson

1. Early analysis suggests that when it comes to quantum computing and quantum communications, the U.S. has shown interest in building the hardware, and China and Japan have been more focused on the applications, software, and use-cases. Global competition in early stages of this race will shape the vendor landscape in future years when quantum communications may have commercial applications. (a) What are the implications in the race to develop and deploy super- and quantum-computing capabilities and quantum communications on a wide scale? (b) Will competitively developing our own systems position us to tackle threats to competition as the technology develops?

Quantum computing and quantum communications are technologies that will revolutionize computing and telecommunications over the next 20 to 30 years. Indeed most federal R&D funding to date has focused on the physics of quantum computing, and recent legislation proposed within the Senate also seems oriented toward further investment in the underlying physics. At this point there is sufficient industry interest in the technology that we will see vendors like IBM and D-Wave make investments that will continue to increase the number of qubits offered by their systems. We are on the cusp of these systems' quantum speedups outpacing conventional computing and surpass Moore's Law.

Investment in applications is critical. If current legislative proposals around quantum research institutes are going to have a meaningful market impact, they must dedicate the majority of their resources into developing algorithms and applications that can leverage emerging quantum computing platforms, and let the promise of these applications drive continued industry investment into the device physics. The Quantum industry is still searching for and seeking to demonstrate the "killer app" that will drive continued investment in the technology.

Regardless of national security concerns, quantum computing is going to exist within a global marketplace. Therefore the US needs to begin investing now in quantum-resistant secure communications technologies. Current solutions like quantum key distribution address this challenge in very limited scenarios, and there needs to be added focus on application-layer public-key cryptography that can stand up to the capabilities of a quantum supercomputer.

The Honorable Chris Collins

- 1. As we heard repeatedly in the testimony, threats not only arise with the equipment out of the box, but often with the long-term access to the equipment by offering ongoing servicing and upgrades. We've also heard that organizations – both the government and private companies – should take a risk management approach to ensuring the security of their networks. What steps can smaller rural providers take to limit their vulnerability?**

While one-size-fits-all compliance approaches can often be unaffordable to smaller operators, risk-based management approaches are inherently designed to scale with the size and resources of the organization, from the large multi-national company all the way down to the individual user. By evaluating risk, small, rural providers can identify the areas where investment in cyber defense can be most meaningful in combating the threat.

A key opportunity for rural providers is participation in emerging cyber threat information sharing communities. The FCC's Communications Security, Reliability and Interoperability Council (CSRIC) studied information sharing and released a report in March 2017 detailing ongoing programs and opportunities for further connectivity through sharing cyber threat information across industry. As these programs mature through venues such as the Telecommunications Information Sharing and Analysis Center (ISAC), the scale and capabilities of larger providers can be brought to bear to support smaller operators.

- 2. In your testimony, you discussed recent changes to the membership of standards bodies which set rules for equipment providers and suppliers. If one country or company sends a disproportionate number of representatives to a standards body, how does that impact the standards body's recommendations? (a) Is it possible for nefarious actors to use their participation in a standards body to influence the outcome in order to create a competitive advantage for their company? (b) With the power standards bodies have to shape the technical foundation of the network devices we use every day, how can we ensure the International standards bodies determine standards based on the best technology, and not the loudest voices? For example, should there be greater transparency or mechanisms to standardize the representation of the members who contribute to these standards bodies?**

Standards bodies are inherently designed for transparency, and their underlying business model presumes that participating organizations, whether companies or governments, are working to advance their own

agendas. These agendas typically revolve around companies seeking to have their intellectual property written into the standards in order for them to garner long-term royalties. As Chinese companies seek to further establish themselves in the global tech economy, having their intellectual property included in standards is a key step. The drivers around this are more economic than seeking to advance a hidden agenda.

The biggest opportunity for the US to maintain a leadership role in standards is for the US Government to increase its role in the standardsmaking process. There has been a considerable decline in participation from organizations such as the National Institute for Standards and Technology (NIST) in standards bodies like the Third Generation Partnership Project (3GPP) and Internet Engineering Task Force (IETF). As foreign countries and companies increase their involvement in standards processes, the best check on that influence would be direct US government participation to help articulate clear priorities.

The Honorable Mimi Walters

1. **DHS, as the Sector Specific Agency for Telecom, is looking into both supply chain risks – including 5G and systemic risks more broadly. The FCC’s CSRIC is also looking into supply chain risks related to 5G. The FCC CSRIC Report is due in September, and the DHS effort may conclude some time later before the end of the year. How do we avoid duplicative or potentially conflicting recommendations from these parallel efforts? Should we vest decision-making authority at one agency?**

There is broad consensus from industry that one agency should take the lead and help coordinate interagency activities to reduce duplicative and potentially conflicting processes. As the Sector Specific Agency for telecommunications, DHS is the logical lead entity to address issues like this.

2. **What level of sophistication does it take to exploit a vulnerability in the physical hardware of this equipment? (a) How does that compare to the sophistication required to exploit the software components? (b) Are either of these threats resolved solely by ripping and replacing vulnerable equipment? (c) Is there a more thoughtful approach you could offer?**

Exploiting vulnerabilities in devices requires discovery of the vulnerability, development of an exploit, and weaponizing that exploit. Generally speaking, it takes more sophistication and resources to discover vulnerabilities in hardware than software, and often discovering hardware vulnerabilities requires the

resources of a nation state actor. Once discovered the sophistication needed to exploit the vulnerabilities is similar.

“Rip and replace” is certainly one approach to dealing with the issue, but represents one extreme on the risk management continuum. For highly-sensitive and/or nationally-critical systems, it may be the right choice.

However for device and systems of lower criticality or lower threat, a range of risk mitigation steps may be more appropriate. For example, in dealing with the potential threat of weaknesses in SS7, industry developed and deployed technology to monitor SS7 infrastructure for malicious use, and if detected use that information to block bad actors from accessing the infrastructure.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

June 1, 2018

Ms. Samm Sacks
Senior Fellow
Technology Policy Program
Center for Strategic and International Studies
1616 Rhode Island Avenue, N.W.
Washington, DC 20036

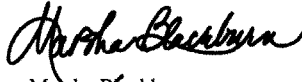
Dear Ms. Sacks:

Thank you for appearing before the Subcommittee on Communications and Technology on Wednesday, May 16, 2018, to testify at the hearing entitled "Telecommunications, Global Competitiveness, and National Security."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, June 15, 2018. Your responses should be mailed to Evan Viau, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed to Evan.Viau@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Marsha Blackburn
Chairman
Subcommittee on Communications and Technology

cc: The Honorable Michael F. Doyle, Ranking Member, Subcommittee on Communications and Technology

Attachment

Additional questions for the record from the May 16, 2018 Subcommittee on Communications and Technology hearing entitled, “Telecommunications, Global Competitiveness, and National Security”

Samm Sacks, Senior Fellow, Center for Strategic & International Studies

The Honorable Marsha Blackburn

1. **China and other competitors have explicitly stated their desire to dominate specific nodes in the supply chain. Given the global nature of the supply chain for information and communication technology, what is our risk?**

There are espionage and economic risks. I leave it to the national security experts to determine the specific threat and how to mitigate it. However, it is difficult to comment on the threat because there is not publicly available information on it. More specific information should be made public so there can be a comprehensive analysis about how to mitigate the threat and what the impact of different measures would be.

- a. **If our competitors were to capture critical nodes in the supply chain, either through market share or through technical prowess, what recourse do we have?**

The United States should not take a sweeping approach that blocks entire companies or discriminates against companies just because they are of a certain national origin. Our policies need to determine the impact of our actions on the U.S. economy, U.S. companies, and our ability to maintain technological leadership and innovate.

2. **It seems that the trusted vendor pool is shrinking each year. If this pace continues, we could find ourselves with only one trusted vendor providing communications infrastructure in the U.S. How can government and industry promote competition and longevity for trusted vendors in the market?**

We must recognize the interdependency of technology and carefully assess the implications for disentangling the United States from global supply chains. Any measures taken against specific competitors should be coordinated efforts with allies and partners to exert international rather than unilateral pressure.

2. **As you note in your work, China uses a command and control approach to orchestrate their national strategies on the supply chain for information technology, emerging technologies, and R&D. The U.S. does not take such an approach; rather, we rely on market-based mechanisms. Can you elaborate on the advantages and disadvantages of command and control, and how the U.S. can leverage the strengths of its market-based approach?**

The Chinese government uses systematic efforts to bolster domestic industry by identifying certain sectors for state support (e.g., by direct subsidy, access to credit or special pricing or other preferential policy treatment). There is also a push for Chinese companies to have a major voice in shaping standards and to expand into global markets.

The semiconductor industry is an example of where decades of state support has not enabled China to develop an indigenous industrial base and reduce reliance on core foreign technologies. On the other hand, Chinese sectors like the digital economy (e.g., ecommerce platforms, financial technology, mobile apps) that are largely commercial and market-driven have demonstrated more success in China. Areas in which China is actually doing the most innovation (at least on the business model, application, and consumer commercial side) are where the government has a much smaller role.

Huawei benefited from massive state subsidies and theft of intellectual property. But the company has been savvy about how it utilized these advantages: its investments in research and development (R&D) and management strategy contributed to building a powerhouse company that now may be the only company in the world capable of making the full range of 5G products that are widely regarded by U.S. and European carriers to be high quality.

The Honorable Mimi Walters

1. DHS, as the Sector Specific Agency for Telecom, is looking into both supply chain risks—including 5G and systemic risks more broadly. The FCC's CSRIC is also looking into supply chain risks related to 5G. The FCC CSRIC Report is due in September, and the DHS effort may conclude some time later before the end of the year. How do we avoid duplicative or potentially conflicting recommendations from all of these parallel efforts?

- a. Should we vest decision-making at one agency?

This is a question which falls outside the scope of my expertise.

The Honorable Tim Walberg

1. When talking about our domestic manufacturing capability, we're also talking about our ability to identify emerging technologies and bring them to commercialization for both U.S. and global markets.

My colleagues have expressed the need for a national strategy that addresses threats to our telecommunications networks, to competition in the supply chain, and to national security. Can you elaborate on how human capital – having a technically trained workforce capable of competing on advanced research and development – plays into such a national strategy?

a. What can Congress do to lead on this piece of the puzzle?

Congress should work to improve the quality of STEM education as well as expanding access to STEM education and training programs. According to a recent study by CSIS, U.S. government spending levels of education are roughly in line with other advanced economies; however, the United States is declining in math and science test scores. There is also significant disparity between low and high incomes students.

Congress should also work to enable incentives for the top researchers and engineers from around the world to work at U.S. labs and research institutes. Beijing has been attracting top talent from around the world to move to China to lead labs by giving them major sources of funding and other forms of support.

Congress also needs to work to prevent racial and ethnic discrimination against researchers based on country of origin. A recent article in Foreign Policy discusses proposed restrictions on Chinese scientists and researchers in the United States. According to the author, 'The United States may feel it's only playing defense in a global cold war over tech. In reality, these policies play into Beijing's preferred vision of the world. China sees science as a tool of national greatness and scientists as servants to the state. This parochial vision discounts the individual agency and ethical obligations of scientists and runs contrary to the cosmopolitan ideal of science. The United States must uphold those ideals, not create new boundaries.'

The Honorable Anna Eshoo

- 1. During my questioning, I asked if anyone had done an analysis on the trusted supply chain to determine whether it is viable for our country to eliminate our dependence on foreign adversarial companies like Huawei and ZTE. You told me it had not, but you would follow up.**

a. Have you or anyone begun to conduct such an assessment?

b. If not, are you willing to do so?

From a commercial lens, Huawei and ZTE equipment has a reputation for being high quality and affordable. In low income rural areas, there really is no viable alternative. Moreover, as we look to 5G, Huawei is perhaps the one company capable of making products across the 5G stack from handsets to network equipment. Reducing dependence on these vendors is therefore difficult.

- 2. Did you agree with the Department of Commerce's decision to implement a seven-year ban on ZTE?**

- a. **If so, should the Department and other U.S. officials investigate whether similar bans are appropriate for other Chinese entities, as Senator Rubio has suggested?**
- b. **Should the Administration continue to indulge ZTE and other companies in 'deals' when we know outright that the company has repeatedly undermined our laws?**

ZTE violated U.S. export control law and resisted compliance with investigations. While it is not uncommon for sanctions against companies to be lifted after a period, the timing and process by which the penalties against ZTE were lifted is highly unusual. These factors—speed and the manner by which messaging and negotiating occurred—undermines the credibility of our sanctions system, sending a message to other governments around the world that law enforcement matters are open to political trading. The fate of ZTE has now become intertwined in a complex web involving trade, supply chain cybersecurity, investment, technological competition that is difficult to untangle.

3. What is the potential for harm to our national security by having foreign adversaries involved in business with U.S. small businesses and start-ups?

There is some risk that China would gain market knowledge or technology through investment in early stage U.S. companies, including in areas with dual-use and national security implications. However, this is not necessarily the case, and depends on two main factors: (1) is the Chinese investor just a passive investor or exercising influence in ways that would give them access to the technology; and (2) is the Chinese investor linked to a strategic or military entity through a shell company structure? Increased resources for CFIUS to monitor these factors is a positive development in capturing risk.

But these factors (access to technology and shell company designed to evade scrutiny) should not be assumed in all cases. That is why it is so critical that the decision be made in a precise manner that identifies real threats, but does not sweep up all Chinese investment under a blanket ban.

There are consequences of overreach and using CFIUS as a blunt instrument for U.S. technological leadership and innovation. Passive investments fund U.S. entrepreneurship, human talent, and innovation in emerging technologies, which are needed to stay ahead of China and others. Chinese funds blocked from U.S. markets would instead go to support innovation in other countries, creating a disadvantage for the United States.

GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641
June 1, 2018

Mr. Clete Johnson
Partner
Wilkinson Barker Knauer, LLP
1800 M Street, N.W.; Suite 800N
Washington, DC 20036

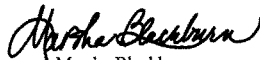
Dear Mr. Johnson:

Thank you for appearing before the Subcommittee on Communications and Technology on Wednesday, May 16, 2018, to testify at the hearing entitled "Telecommunications, Global Competitiveness, and National Security."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on Friday, June 15, 2018. Your responses should be mailed to Evan Viau, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed to Evan.Viau@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Marsha Blackburn
Chairman

Subcommittee on Communications and Technology

cc: The Honorable Michael F. Doyle, Ranking Member, Subcommittee on Communications and Technology

Attachment

WILKINSON) BARKER) KNAUER) LLP

1800 M STREET, NW
SUITE 800N
WASHINGTON, DC 20038
TEL 202.783.4141
FAX 202.783.6851
WWW.WBKLaw.COM
CLETE D. JOHNSON
202.383.3406
CJOHNSON@WBKLAW.COM

June 15, 2018

Evan Viau
Legislative Clerk
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Re: *Responses to Questions for the Record*

Dear Evan:

In response to Chairman Marsha Blackburn's request of June 1, 2018, please find attached my answers to the additional questions from Members of the Subcommittee on Communications and Technology following the hearing on May 16, 2018 entitled "Telecommunications, Global Competitiveness, and National Security."

It was an honor to testify at the hearing, and as noted in my attached answers to Members' questions, I would be happy to follow up on these important issues if they or their staff personnel have any further questions on which I may be of assistance.

Sincerely,



Clete D. Johnson

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

Responses to Questions for the Record

Clete D. Johnson
 Partner, Wilkinson Barker Knauer LLP

**Hearing on Telecommunications, Global Competitiveness, and National Security
 May 16, 2018**

**House Committee on Energy and Commerce
 Subcommittee on Communications and Technology**

The Honorable Pete Olson

Some might say that the U.S. is already “catching up” with other nations in the race to 5G. Whether or not that is an accurate assessment, there are many more nascent technologies that are still in the early stages of development, such as AI, autonomous vehicles, robotics, and biotech to name a few. How do we ensure that the U.S. remains a competitive force in these fields while also guarding against national security threats?

Over the long term, boosting consumer and business confidence in the security of U.S. networks and their constituent equipment and services will play a crucial role in keeping the United States ahead of the competitive curve in all of these areas.

Secure, reliable networks built through trusted suppliers of equipment and services are the key to this future market leadership. The U.S. government and a broad collection of industry stakeholders have undertaken collaborative efforts toward innovation among trusted suppliers and a secure and vibrant internet and communications ecosystem through many policy and standards processes. For instance, initiatives led by the Departments of Commerce and Homeland Security under Executive Orders 13636 and 13800, along with international efforts such as the Common Criteria for Information Technology Security Evaluation, the Open Group Trusted Technology Forum, and the International Standards Organization, have provided avenues to advance both innovation and security.

As we develop methods to identify and promote competition among trusted suppliers, we must also identify suppliers whose corporate structures, personnel, and relationships with adversary governments and intelligence services are particularly susceptible to tactical or strategic exploitation. This is the focus of significant recent policy activity in the Executive Branch and in Congress. Going forward, the Department of Homeland Security (DHS), as the Sector Specific Agency for both the communications and the IT sectors, should coordinate these efforts through thorough interagency processes that take in pertinent information from expert government agencies such as the Departments of Defense, Commerce, and State, and the FBI and other appropriate elements of the law enforcement and intelligence communities. The actions of the Federal Communications Commission (FCC) and other regulatory authorities should also be coordinated within these broader processes. Additionally, to promote collaborative and candid

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

partnership with the industry stakeholders who know these markets best, sensitive private sector information provided to the government by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits both public disclosure of protected information and use of such information in civil litigation or regulatory rulemaking or enforcement actions. Over the longer term, formal supply chain security determinations regarding which suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions should derive from these broader interagency processes or related statutory requirements.

The Honorable Bill Johnson

Early analysis suggests that when it comes to quantum computing and quantum communications, the U.S. has shown interest in building the hardware, and China and Japan have been more focused on the applications, software, and use-cases. Global competition in the early stages of this race will shape the vendor landscape in future years when quantum communications may have commercial applications.

- a) *What are the implications in the race to develop and deploy super- and quantum-computing capabilities and quantum communications on a wide scale?*
- b) *Will competitively developing our own systems position us to tackle threats to competition as the technology develops?*

As discussed in the hearing, I believe that collaborative and multistakeholder efforts like those undertaken by the Department of Commerce – particularly the quantum computing work conducted by the scientists of the National Institute of Standards and Technology (NIST), along with leading academic and industry experts – can allow for transformative breakthroughs in security, computing, and communications. The key to harnessing the potential of these advances is for the U.S. government to use its convening authority, along with funding and other support for basic research, to allow U.S. innovators to flourish. In contrast, centrally-planned, top-down government industrial policy may be the approach of autocratic governments such as China's, but it is not the best approach for the United States to achieve the full potential of our uniquely innovative society.

The Honorable Chris Collins

As we've heard repeatedly in the testimony, threats not only arise with the equipment out of the box, but often with the long-term access to that equipment by offering ongoing servicing and upgrades. We've also heard that organizations – both the government and private companies – should take a risk management approach to ensuring the security of their networks. What steps can smaller, or rural, providers take to limit their vulnerability?

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

The challenge of supply chain security is perhaps most acute for smaller providers that operate with lower margins and less capital resources and staff than larger national providers.

As discussed in the hearing, the Federal Communications Commission (FCC) has begun a formal rulemaking process proposing to prohibit Universal Service Fund (USF) support for purchases of equipment and services from companies that pose a national security threat to the United States' communications infrastructure. This proposal cites three companies: Huawei, ZTE, and Kaspersky Lab. This notice-and-comment rulemaking process is producing the first-ever substantial and detailed public record on these issues. The 23 comments submitted in the first round of comments in this proceeding, submitted on June 1, collectively contain significant discussion of the market considerations pertaining to a possible prohibition of Huawei and ZTE from the USF-supported market; the reply round of comments, due July 2, is expected to further flesh out the record regarding this market.

While the rules that may result from this proceeding could ultimately disrupt the present supply chains of certain providers to some extent, the record that is developing through this notice-and-comment process may be particularly valuable in finding creative and cost-effective solutions to the challenges that confront small providers in particular. For instance, the newly intense focus on these supply chain security issues may illuminate new possibilities for further developing information sharing capabilities, government assistance partnerships, and collaborative relationships with larger peering partners beyond those that exist today. I would be happy to follow up with your staff in further detail following the completion of this record.

The Honorable Mimi Walters

DHS, as the Sector Specific Agency for Telecom, is looking into both supply chain risks – including 5G and systemic risks more broadly. The FCC's CSRIC is also looking into supply chain risks related to 5G. The FCC CSRIC Report is due in September, and the DHS effort may conclude some time later before the end of the year. How do we avoid duplicative or potentially conflicting recommendations from all of these parallel efforts?

a) Should we vest decision-making at one agency?

The Department of Homeland Security (DHS), as the Sector Specific Agency for both the communications and the IT sectors, should coordinate thorough interagency processes on supply chain security that take in pertinent information from expert government agencies such as the Departments of Defense, Commerce, and State, and the FBI and other appropriate elements of the law enforcement and intelligence communities. The actions of the Federal Communications Commission (FCC) and other regulatory authorities should also be coordinated within these broader processes. Additionally, to promote collaborative and candid partnership with the industry stakeholders who know these markets best, sensitive private sector information provided to the government by individual companies should be formally protected under the Protected Critical Infrastructure Information Act, administered by DHS, which prohibits both public disclosure of protected information and use of such information in civil litigation or regulatory

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

rulemaking or enforcement actions. Over the longer term, formal supply chain security determinations regarding which suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions should derive from these broader interagency processes or related statutory requirements.

The Honorable Anna G. Eshoo

1. *During my questioning, I asked if anyone had done an analysis on the trusted supply chain to determine whether it is viable for our country to eliminate our dependence on foreign adversarial companies like Huawei and ZTE. You told me it had not, but you would follow up.*
 - a) *Have you or anyone begun to conduct such an assessment?*
 - b) *If not, are you willing to do so?*

While I am not aware of a publicly available analysis that directly answers this question, there are multiple pertinent government-industry processes underway that may begin to provide the foundation for such an analysis.

First, the Federal Communications Commission (FCC) has begun a formal rulemaking process proposing to prohibit Universal Service Fund (USF) support for purchases of equipment and services from companies that pose a national security threat to the United States' communications infrastructure. The notice for this proposed rulemaking cites three companies: Huawei, ZTE, and Kaspersky Lab. This notice-and-comment rulemaking process is producing the first-ever substantial and detailed public record on these issues. The 23 comments submitted in the first round of comments in this proceeding, submitted on June 1, collectively contain significant discussion of the market considerations pertaining to a possible prohibition of Huawei and ZTE from the USF-supported market; the reply round of comments, due July 2, is expected to further flesh out the record regarding this market.

Also, the FCC has tasked its Communications Security, Reliability and Interoperability Council (CSRIC), a formal Federal Advisory Committee of private sector and other experts, to conduct a study to "identify and examine the security risks to the emerging 5th generation [5G] wireless networks." Among other tasks, the CSRIC has been asked to provide recommendations to address "vulnerable supply chains." The CSRIC report for this 5G-focused effort is due in September. While this effort is aimed primarily at developing "best practices for the design, deployment, and operation of risk-tolerant 5G networks to mitigate the identified risks," rather than a purely market-oriented analysis of specific suppliers, the public findings and recommendations in this report will augment the public record that will have been created through the separate FCC rulemaking process mentioned above.

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

Additionally, the Department of Homeland Security (DHS) has begun a program of Telecommunications Supply Chain Risk Assessments that will consist of both general assessments of the sector's supply chain risks and targeted assessments of specific threats, vulnerabilities and entities at risk. The general risk assessment is expected to be completed and published by August 31, and the targeted assessments will begin thereafter.

Meanwhile, the Commerce Department's National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) continue multiple workstreams, respectively, for developing supply chain risk management guidance and conducting policy analysis and multistakeholder consensus building for internet and communications ecosystem best practices.

All of these processes are advancing our understanding of these issues and will provide new publicly available information to augment other government, private sector, and academic studies of more discrete components of this market challenge. In particular, following the submission of reply comments in the FCC's rulemaking proceeding on July 2, there will likely be a public record sufficient to begin the market analysis that you are seeking. Of course, if you wish, I would be happy to explore further with your staff the available public resources for, and the possible parameters and methodologies of, such an analysis.

2. *Did you agree with the Department of Commerce's decision to implement a seven-year ban on ZTE?*
 - a) *If so, should the Department and other U.S. officials investigate whether similar bans are appropriate for other Chinese entities, as Senator Rubio has suggested?*
 - b) *Should the Administration continue to indulge ZTE and other companies in 'deals' when we know outright that the company has repeatedly undermined our laws?*
 - c) *What is the potential for harm to our national security by having foreign adversaries involved in business with U.S. small businesses and start-ups?*

ZTE's scheme to evade U.S. export controls was an egregious violation of laws that protect our national security. The law enforcement actions pertaining to ZTE's illegal activities and its reported violations of the 2017 settlement agreement – including any additional penalties or subsequent settlement agreements that may be appropriate – should be treated purely as law enforcement actions, separate and distinct from policy decisions or policy-related negotiations.

Regarding additional prohibitions beyond the existing export denial order against ZTE, as you well know, there are certain existing statutory prohibitions against federal procurement of ZTE, Huawei, and Kaspersky Lab. Pending legislation in Congress would expand these prohibitions against ZTE and Huawei, and possibly include altogether new statutory prohibitions against three video equipment companies. Beyond these companies that have been the subject of

Clete D. Johnson
 Wilkinson Barker Knauer LLP
 Responses to Questions for the Record

statutory bans and/or related legislative attention, the FCC and DHS processes mentioned above should seek to establish thoroughly well-coordinated interagency processes, led by DHS as the Sector Specific Agency for the communications and IT sectors, that take in relevant information from expert government agencies and private sector stakeholders to determine which if any other suppliers or particular equipment or services should be subject to special security scrutiny, restrictions or prohibitions. Over the longer term, any such action should derive directly from these broader interagency processes or statutory requirements.

Finally, regarding the question about foreign adversaries' targeting of small businesses and start-ups, this part of the market can be fertile ground for adversaries' infiltration and espionage. As you well know, the technological advances in Silicon Valley and other innovation hubs is one of the United States' greatest strategic assets. Adversaries' infiltration and/or theft of these companies' proprietary business processes and intellectual property is a serious strategic national security concern.

3. *What would be the costs to U.S. industry be to comply with laws that would prevent companies from using Huawei or ZTE equipment or equipment produced in China?*
 - a) *What would be the costs to U.S. industry of replacing Huawei or ZTE equipment that may be on their networks?*
 - b) *What would be the costs to U.S. industry of complying with laws that would prevent companies from using Huawei or ZTE equipment or equipment produced in China?*
 - c) *What would be the costs to U.S. industry of complying with laws that would prevent companies from using Huawei or ZTE equipment or other equipment produced in China?*

As discussed above in Question 1, the multiple ongoing government-private sector processes will provide new publicly available information to address these cost/benefit questions. In particular, the FCC's rulemaking proceeding (reply comments due July 2) is creating the first substantial and detailed public record on these issues, and that record will provide a base of information from which to derive answers to these questions. As with the market analysis you requested at the hearing and in Question 1 above, I would be happy to develop answers to these questions with the benefit of the full record in the FCC proceeding, following the July 2 submission of reply comments.