**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

RPTR TELL

EDTR ZAMORA

TELECOMMUNICATIONS, GLOBAL COMPETITIVENESS,

AND NATIONAL SECURITY

WEDNESDAY, MAY 16, 2018

House of Representatives,

Subcommittee on Communications

and Technology,

Committee on Energy and Commerce,

Washington, D.C.

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.

Present: Representatives Blackburn, Lance, Shimkus, Latta, Guthrie, Kinzinger, Bilirakis, Johnson, Long, Flores, Brooks, Collins, Walters, Costello, Walden (ex officio), Welch, Clarke, Loebsack, 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, Minority Counsel; Dan Miller, Minority Policy Analyst; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; 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.

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 outmaneuver 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.

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

[The prepared statement of Mrs. Blackburn follows:]

******** COMMITTEE INSERT ********

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.

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

[The prepared statement of Mr. Lance follows:]

******** COMMITTEE INSERT ********

Mrs. Blackburn. The gentleman yields back.

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

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.

[The prepared statement of Ms. Clarke follows:]

******** COMMITTEE INSERT ********

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

Mr. Walden, you are recognized.

The Chairman. 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 face similar questions as our adversaries appear 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 reverse. 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.

With that, Madam Chair, unless any members on the Republican side want the

remainder of my time, I would be happy to yield back.

[The prepared statement of Chairman Walden follows:]

******** COMMITTEE INSERT ********

Mrs. Blackburn. The gentleman yields back.

Mr. Pallone, you are recognized for 5 minutes.

Mr. Pallone. Thank you, Madam 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 bittersweet 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.

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

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

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, Mr. Clancy. You are now recognized for 5 minutes for your statement.

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

**STATEMENT OF CHARLES CLANCY**

Mr. 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 Mr. Clancy follows:]

******** INSERT 1-1 ********

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 want to discuss three implications for U.S. ICT companies doing business with China.

Mrs. Blackburn. Excuse me. Ms. Sacks, would you speak directly into the microphone? Thank you.

Ms. Sacks. 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:]

******** INSERT 1-2 ********

Mrs. Blackburn. The gentlelady yields back.

Mr. Johnson, you are recognized for 5 minutes.

**STATEMENT OF CLETE JOHNSON**

Mr. Johnson. Thank you.

Madam Chairman, distinguished --

Mrs. Blackburn. Turn your mike on. Your microphone, please.

Mr. Johnson. Oh, sorry.

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 interagency 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:]

******** INSERT 1-3 ********

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. Okay. 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 engagement. 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?

Mr. 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?

Mr. 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?

Mr. 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?

Mr. 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?

Mr. 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 is what we are seeing, here is what I am picking up, and here is what my concerns are, and here is 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.

Mr. 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?

Mr. 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 role provider that relies on these kinds of services manage these kinds of threats?

Mr. 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?

Mr. 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. Okay. Well, thank you. Madam Chair, my time has expired. I yield back.

Mrs. Blackburn. The gentleman yields back.

Mr. Loebsack, 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 is 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.

RPTR DEAN

EDTR ZAMORA

[11:00 a.m.]

Mr. Loebsack. 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.

Mr. 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.

Mr. 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 website 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, D.C., which has made into the open source. Are you aware of reports that DHS has detected the presence of these devices in the greater D.C. area?

Mr. 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?

Mr. 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 activity 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 D.C. 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 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 -- two Russian -- 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 an 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. -- needs to have public information, it cannot be classified --

Ms. Eshoo. Just a second. We know -- we know from -- 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 way 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?

Mr. 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.

Mr. 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 have -- 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 communications 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 again 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.

Mr. 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. Okay. 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?

Mr. 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. Okay. Ms. Sacks, do you agree?

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

Ms. Matsui. Okay. 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, okay. 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. Okay. 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?

Mr. 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 --

Mr. 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 is 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 certainty 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?

Mr. 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?

Mr. 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. Okay, 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 Jingping'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. Okay, thank you.

And, Madam Chairman, I would like to submit an article for the record, U.S. 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 follows:]

**This is a preliminary, unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker. A link to the final, official transcript will be posted on the Committee's website as soon as it is available.**

******** COMMITTEE INSERT ********

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.

Mr. 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 IT 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?

Mr. Clancy. Specifically with respect to their use of --

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

Mr. Clancy. So, I mean, in the standard bodies that I have been involved in, it has been basically the more internet Ciscos and Qualcomms 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. Okay. 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 do 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.

Mr. 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.

RPTR TELL

EDTR ZAMORA

[12:00 p.m.]

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'Reilly, a U.S.-China Commission Report, articles by Samm Sacks and Andrew Hunter of CSIS, two Wall Street Journal articles, and the ZTE denial order, and one article from The Hill.

Without objection, so ordered.

[The information follows:]

******** INSERT 1-4 ********

Mrs. Blackburn. 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.]