S. Hrg. 116–185

SUPPLY CHAIN SECURITY, GLOBAL COMPETITIVENESS, AND 5G

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

OCTOBER 31, 2019

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
40–385 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
MICHELLE D. WOODS, *Director of Homeland Security*
MICHAEL J.R. FLYNN, *Senior Counsel*
DAVID M. WEINBERG, *Minority Staff Director*
ALEXA E. NORUK, *Minority Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Minority Fellow*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

THURSDAY, OCTOBER 31, 2019

ALPHABETICAL LIST OF WITNESSES

APPENDIX

SUPPLY CHAIN SECURITY, GLOBAL COMPETITIVENESS, AND 5G

THURSDAY, OCTOBER 31, 2019

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 9:32 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Lankford, Romney, Scott, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing is called to order.

I want to welcome all the witnesses. Thank you for your thoughtful written testimony, and we are looking forward to hearing your oral testimony and answers to our questions.

I would ask that my written statement be entered into the record.[1]

I just want to make a couple comments about kind of what I want to see the goal of this hearing to be, which is very similar to pretty much the goal of every hearing as a basic problem-solving process.

I will start out. I have not done this in a while, but this Committee, under my chairmanship, developed a mission statement "to enhance the economic and national security of America and promote more efficient, effective, and accountable government."

The reason I am pointing it out today is I cannot really think of a hearing where that mission statement is more applicable to. When we start talking about 5G, we are talking about the economic opportunity, but we are talking about the national security risks. In order to take advantage of that opportunity, in order to avoid those national security risks, we need more efficient and effective government to step up to the plate to compete against what, unfortunately, is becoming not just a friendly economic rival but an adversary and somewhat of, in many cases, a maligned actor on the world stage, China.

So, in terms of the definition of this problem—and, again, I am really hoping to be able to lay out a simplified definition, lay out

[1] The prepared statement of Senator Johnson appears in the Appendix on page 47.

some priorities of things we need to address, so that it can focus everybody's attention on this.

So let me take a stab at the problem definition. This is an unusual one because it really starts as an opportunity. It is an opportunity of moving from 4G to 5G, which globally that will be trillions of dollars' worth of economic activity. So it is an enormous opportunity, and, of course, there is going to be a great deal of competition to take advantage of that opportunity.

The problem really rests if we do not take advantage of it, if we are not a leader, other people set the standards, and again, those other people, primarily the threat would be in China, not setting the standards that really contribute to a free and open society.

We have the economic aspects of this. We have to set the standards. The threat that China poses in terms of just intellectual property theft—one of the reasons they can compete with us on 5G is because they have stolen hundreds of billions of dollars' worth of our intellectual property. Now they are threatening to leapfrog us from that standpoint.

So, again, the actions, based on that basic problem definition, that opportunity that also is a problem, we have to address the spectrum allocation in at least two different types of bands. We have a great witness from the Federal Communications Commission (FCC) that can really talk to us about that.

We need to be involved and hopefully be a leader in setting the standards. We need to look at a trusted supply chain, and then where there is not proper market activity—and I hate to say this, but we are competing against a nonmarket economy, a command economy, a very strategic competitor. We may have to take a look at market breakdowns here and do something from the standpoint of government to make sure that we support the type of supplier base that we are going to need.

So, again, that is kind of my relatively simple, off-the-top-of-my-head definition of what this problem is and some of the top priorities.

Again, I read all the testimony and really appreciate it. I just encourage everybody to try and simplify this as much as possible so that we leave this hearing with a pretty good understanding of what we are facing and the first steps that we have to take.

One final comment—and, Diane, I think you were in that secure briefing which was called probably about a month ago, and I know my input in that was "OK. Now who is in charge of this effort?" I am heartened by the fact that in testimony, we definitely have an answer. It is literally the National Economic Council (NEC), residing in the White House. I spoke with Larry Kudlow last night. He has been actively engaged, and I was really glad to hear that, together with the Chairman of the FCC and with active involvement with President Trump as well.

So this is a high priority. It is taken that way. I think we have the—who is in charge of this effort, and certainly, what we have heard in that secure briefing is we have the interagencies working very cooperatively.

We have that final piece that I was wondering. It is great that everybody is working cooperatively together, all the component experts, but now, at least for my satisfaction, I have identified this

is the agency. This is the individual that really is in charge of this and also could be held accountable for what these goals, what these actions need to be that we need to take.

So, again, I am already heartened by just going through the briefing, what I have heard, what I have read, coming to this hearing, and I am really looking forward to the hearing itself and hopefully gain a little bit more confidence that we are not behind, as I thought we were. We are actually getting up in pretty good position and, I think, poised to hopefully leap ahead and actually win this competition.

So, with that, Senator Peters.

OPENING STATEMENT OF SENATOR PETERS[1]

Senator PETERS. Thank you, Mr. Chairman, and thank you to all of our witnesses for being here today.

Our modern economy is truly global. Internet access is no longer a luxury. It is necessary and a vital tool that connects people with educational opportunities. It creates jobs, drives economic development.

The introduction of 4G technology brought us live streaming, ridesharing, on-demand delivery, and other innovations, and now 5G era is before us.

This faster, strong, wireless connection will once again transform our digital world, enabling new technologies like precision agriculture, self-driving cars, and augmented reality.

5G networks and the new technologies they spur will create countless new jobs in Michigan and generate billions of dollars in economic growth all across our country. 5G has the potential to unleash new productivity and help cement the United States as a global leader in innovation, but developing the infrastructure needed to support 5G networks across the country does not come without risks.

Today China, arguably our Nation's greatest global competitor, is poised to lead the world in advancing this very important technology. China's edge in the development of 5G equipment and standards poses a threat to both American economic dominance as well as our national security. The United States is increasingly reliant on high-speed telecommunications services to support not only our broader economy, but also our defense industry.

In the face to expand 5G access, we face serious supply chain security risks by purchasing and deploying Chinese-made equipment from companies like Huawei and Zhongxing Telecommunication Equipment (ZTE), companies that our intelligence community (IC) has said are beholden to the Chinese government.

The devices these companies provide potentially offer cost-effective solutions to help close the digital divide, but they also pose a serious national security risk and could open a back door into critical American security networks.

Given these serious national security risks, we must navigate a very delicate balance of ensuring that emerging 5G networks are both secure and widely available in both rural and urban areas.

---

[1] The prepared statement of Senator Peters appear in the Appendix on page 49.

China's advantage in 5G may be a reality for now, but it is something we have the power to change. The U.S. Government, including this Committee, has an opportunity to play a key role in America's resurgence as a leader in the development of 5G networks. A challenge of this magnitude requires a strong, unified, and collaborative approach, capitalizing on the full power of American ingenuity.

But, to date, our efforts have been piecemeal and disorganized. We have not had dedicated leadership or the coordinated national strategy needed to accomplish this very critical mission.

I am encouraged by the bipartisan agreement this Committee has made to support this goal. Universal 5G connectivity would encourage renewed prosperity in both urban and rural communities, unlock tremendous economic growth, and reestablish America as the leader in global innovation.

I hope this hearing will serve as a driving force to help us usher in this new age and build momentum toward recapturing our place as the world's leader in communication technologies.

I look forward to the testimony of our witnesses. Thank you for being here today.

Chairman JOHNSON. Thank you, Senator Peters.

It is the tradition of this Committee to swear in witnesses, so if you will all stand and raise your right hand.

Do you swear the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. KREBS. I do.

Ms. RINALDO. I do.

Mr. STRAYER. I do.

Ms. ROSENWORCEL. I do.

Chairman JOHNSON. Please be seated.

Our first witness is Chris Krebs. Mr. Krebs currently serves as the Director of the Cybersecurity and Infrastructure Security Agency (CISA). Previously, Mr. Krebs worked within the Department of Homeland Security (DHS) as a senior advisor to the Assistant Secretary for the Infrastructure Protection, where he helped establish a number of national and international risk management programs. Prior to joining the Department of Homeland Security, Mr. Krebs was the Director of Cybersecurity Policy for Microsoft, leading their work on cybersecurity and technology issues. Mr. Krebs.

TESTIMONY OF THE HONORABLE CHRISTOPHER C. KREBS,[1] DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Good morning, Chairman Johnson, Ranking Member Peters, and Members of the Committee. Thank you for holding today's hearing and providing me an opportunity to be the first government witness to congratulate the world champion Washington Nationals and on behalf——

[Applause.]

Gotcha. Thank you.

[1] The prepared statement of Mr. Krebs appear in the Appendix on page 51.

I also ask the Lerner family to lock up Stephen Strasburg in a lifetime contract.

I also appreciate the opportunity to testify regarding the Cyber and Infrastructure Security Agency's ongoing efforts to secure the supply chain of information and communications technology, including 5G, the next generation of mobile communications networks.

This is a timely hearing. No, not because it is Halloween, and this is often touted as a scary topic with boogeymen hiding behind every line of code or microchip, but because today is the last day of National Cybersecurity Awareness Month and because tomorrow marks the first day of Critical Infrastructure Security and Resilience Month.

While my written testimony details CISA's broader approach to information and communications technology, supply chain, and risk management, I would like to focus my opening remarks on the administration's efforts to secure 5G networks.

As agencies, we have been hard at work on supply chain and 5G security for years now, taking advantage of the respective authorities, roles, and responsibilities of the various Executive Branch departments and agencies, a few represented here today.

Over the last year, our administration-wide strategy has really come together, all under the guidance of the National Economic Council and the National Security Council (NSC).

While there is no department of 5G, no department of supply chain security, and nor should there be, I can say with confidence that the U.S. Government is collaborating effectively across the interagency and with our industry partners.

We have tight coordination mechanisms to drive the security and resilient results we all desire. Our goal is pretty straightforward. We seek to foster a competitive global ecosystem for trusted 5G vendors and promote a risk-based approach to 5G.

In part, this will unlock American innovation and provide untold opportunities in the development of tomorrow's technologies. More importantly, it will deliver secure and resilient telecommunications systems and provide a sound base for 5G-enabled technologies.

Our approach has four primary work streams, and I will briefly touch on the work streams and allow my colleagues to expand, as appropriate.

First, we are addressing the policy and regulatory considerations, domestically and abroad, stressing open interoperable systems with respect to the rule of law and taking into account risks posed by the undue influence of foreign governments on suppliers.

Second, we are examining the underpinning technology requirements, including the changes that are anticipated with software-defined networking, virtualization, and the resulting impacts on enabled services and features, like autonomous vehicles, telemedicine, smart cities, and so on.

Next, our work in the economic space focuses on the incentives needed to support growth of new technologies, with an emphasis on a flourishing vendor base here in the United States, while also encouraging global financial practices, subsidies, investments, financing that are open, fair commercially reasonable, and transparent.

Finally, we seek to promote secure and resilient systems, developing a better understanding of where risk lies in our networks and managing that risk accordingly.

CISA is focused here, seeking to support a risk-based approach. Our approach is consistent with our broader supply chain risk management philosophy, encompassing technical, legal, and relationship aspects of a product, company, and the regime from where the product originates.

Specifically, CISA intends to address 5G security concerns through three primary avenues, all of which are core agency competencies: technical evaluation and analysis, stakeholder engagement, and cybersecurity best practices. We recognize that although 5G is a new and transformative technology, the essential elements to future security remain rooted in the way CISA secures all its equities.

I would also like to reinforce that this is not solely a U.S. Government undertaking. Our partners in industry are critical in driving real advances in security and privacy by design and deployment, accompanied by the transparency necessary to inform appropriate risk management decisions by industry and consumers alike.

Efforts like the Council to Secure the Digital Economy's Consensus Baseline Internet of Things (IoT) Security Capabilities as well as the Charter of Trust are both examples of industry-driven consensus efforts to help achieve that global competitive ecosystem for trusted vendors and componentry.

As the director of CISA, with a mission that analyzes risk holistically across 16 critical infrastructures and 55 national critical functions, my commitment to you all is to continue leading, coordinating, and catalyzing these activities for our mutual benefit. More work needs to be done. That is clear, but I believe we have the structures, people, and imperatives to get the job done.

That is the goal. It is now up to a wide group of stakeholders, both public and private, to ensure its realization.

Once again, thank you for the opportunity to appear today, and I look forward to your questions.

Chairman JOHNSON. Thank you, Mr. Krebs.

Even though the Nationals did knock the Brewers out of the playoffs, that was a really fun game to watch, and I congratulate them as well.

Our next witness is Diane Rinaldo. Ms. Rinaldo is the acting Assistant Secretary for Communications and Information for the Department of Commerce. Prior to joining the Department, Ms. Rinaldo was with the House Permanent Select Committee on Intelligence, where she was the lead committee staffer on Congress' landmark cybersecurity legislation, the Cybersecurity Act of 2015. Ms. Rinaldo also previously served as the oversight and budget monitor for the National Security Agency. Ms. Rinaldo.

TESTIMONY OF DIANE RINALDO,[1] ACTING ASSISTANT SECRETARY, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE

Ms. RINALDO. Chairman Johnson, Ranking Member Peters, Members of the Committee, thank you for the opportunity to testify today on supply chain, global competitiveness, and 5G.

The National Telecommunications and Information Administration (NTIA) is responsible for advising the White House on telecommunications and information policy. In consultation with other Commerce bureaus and the Executive Branch agencies, NTIA advocates for domestic and international policies that preserve the open Internet and advance key U.S. interests at home and abroad.

Our role is to foster national security, economic prosperity, and delivery of the critical public services through telecommunications. We are involved in a host of policy issues that affect the security of critical elements in our Nation's telecommunications infrastructure.

Winning the race to 5G is one of the most urgent areas of focus for NTIA, the Department, and the Administration. We are pursuing policies that enable government and industry to work together to deliver on the promises of secure 5G networks.

But as Secretary of Commerce Wilbur Ross has said, we cannot be complacent. Although the United States leads the world in the application of 4G wireless technologies, other countries are trying hard to position themselves to dominate the next generation of 5G technology and services.

Given the global nature of the telecommunications industry, the fight for 5G dominance will center around key issues, including the development of industry standards as well as the ability to win in non-U.S. markets.

NTIA is working closely with the State Department, Homeland Security, the Department of Defense (DOD), and the Federal Communications Commission on policies to secure the supply chain for critical information and communications technologies, enable secure network deployment, and promote innovation and free-market principles.

Our increased reliance on connectivity comes with increased vulnerability to cyberattacks. Securing our networks must be a major priority. We must incorporate prevention, protection, and resiliency from the start.

One of the top priorities for the Administration is securing the information technology (IT) and communications supply chain, which is increasingly vulnerable to certain foreign-sourced products and services.

At the most basic level, we must avoid clear risks. Technology that comes from suspect origins or practices should not be put into our critical systems. At NTIA, we are working to increase transparency across the digital ecosystem to help organizations make better decisions and reduce cybersecurity risks and incidents.

NTIA is helping to address these challenges by supporting the Secretary of Commerce in implementing the President's Executive

[1] The prepared statement of Ms. Rinaldo appears in the Appendix on page 60.

Order (EO) on Securing the Information and Communications Technology and Services Supply Chain.

NTIA has led three recent and successful multi-stakeholder processes on cybersecurity, looking at the challenges around disclosing software vulnerabilities and patching insecure devices.

NTIA is also involved in an ongoing effort to mitigate the damaging effects of botnets.

In our competitive world, the United States does not have the luxury of pursuing only some of our national priorities that depend on spectrum. We must pursue and achieve all of them.

We will continue to build on the excellent model of coordination NTIA has developed with its Federal and private-sector partners.

Again, thank you for inviting me today, and as Chris said, go Nats.

Chairman JOHNSON. Thank you, Ms. Rinaldo.

Our next witness is Rob Strayer. Mr. Strayer is the Deputy Assistant Secretary for Cyber and International Communications and Information Policy at the State Department. In this capacity, he leads the development of international cybersecurity, Internet, data, and privacy policy. Earlier in his career, Mr. Strayer served as the General Counsel (GC) to the U.S. Senate Foreign Relations Committee and deputy chief staff director for U.S. Senate Committee on Homeland Security and Governmental Affairs.

Mr. Strayer, welcome back.

TESTIMONY OF ROBERT L. STRAYER,[1] DEPUTY ASSISTANT SECRETARY FOR CYBER AND INTERNATIONAL COMMUNICATIONS AND INFORMATION POLICY, U.S. DEPARTMENT OF STATE

Mr. STRAYER. Thank you. Thank you, Mr. Chairman, Ranking Member Peters, and Members of the Committee. It is truly a privilege to testify before a committee where I served as a staffer a decade ago.

As the world becomes more interconnected, the security of our information and communications technology, including the fifth generation of wireless technology, is becoming increasingly important for our national security and economic prosperity, as well as the protection of privacy and individual liberties around the world.

The State Department, under Secretary Pompeo's leadership, is in charge of the United States' international engagement campaign to convince our allies and partners of the importance of adopting measures to secure their 5G networks. As you both have noted, 5G networks will be transformative. They will empower a vast array of new services, including traditional critical infrastructure, like the distribution of electricity.

With all these services relying on 5G networks and the masses amounts of personal data that they will provide, the stakes could not be higher for securing these networks.

As countries around the world upgrade their communication systems to 5G technology, we are urging them to adopt a risk-based security framework.

[1] The prepared statement of Mr. Strayer appears in the Appendix on page 66.

I have been joined by colleagues from the full interagency in probably hundreds of bilateral and multilateral meetings over the last, almost 2 years now. I personally have done many dozens of trips focused on 5G. I spent the Labor Day weekend, in fact, with Chairman Pai visiting three countries in the Gulf Region, including Saudi Arabia and Bahrain as well as going to Germany. So we have a full-court press to educate our partners about the security risks and ways that they can achieve a successful future with 5G.

An important element of the 5G security approach that we recommend is a careful evaluation of hardware and software equipment vendors. The evaluation criteria should include the extent to which vendors are subject to control by a foreign government, with no meaningful checks and balances on its power to compel cooperation of those vendors with intelligence and security agencies.

While this should be applied to vendors in all countries, our current concern is primarily with equipment vendors from the People's Republic of China (PRC). Our assessment is that the PRC could compel Chinese equipment vendors to act against the interests of U.S. citizens and citizens of other countries around the world.

If allowed to construct and service 5G networks, Chinese equipment vendors will be in a privileged position in these critical networks. They can be required by China's national intelligence law to cooperate with Chinese intelligence and security services and to keep that cooperation secret, and there is no independent judiciary or rule of law to prevent them from being required to take those actions.

This will provide Chinese Communist Party the capability to disrupt critical infrastructure, intercept sensitive transmissions, and acquire sensitive technology and intellectual property as well as the information of private citizens.

Not only will China have these capabilities, but it has already demonstrated its intent to misuse and exploit data. Chinese technology firms are working with authoritarian regimes often hand-in-hand with the Chinese government to suppress freedom of expression and other human rights through mass arbitrary surveillance, censorship, and targeted restrictions on Internet access. They have exported facial recognition technology that they have perfected in the Xinjiang Province to more than a dozen countries.

The PRC and Chinese firms also have a long history of intellectual property theft to benefit their interests. We should not allow 5G to be yet another vector for the PRC to steal intellectual property.

Through our engagement, many other countries are now acknowledging the supply chain security risk and beginning to strengthen their 5G networks alongside the United States.

For example, Australia, Japan, and Taiwan have taken very specific actions to protect their 5G networks from untrusted suppliers, and in May, the Czech Republic hosted more than 140 representatives of 32 countries from around the world as well as the European Union (EU) and North Atlantic Treaty Organization (NATO) to build consensus on a common approach to 5G security.

This effort produced what is known as the Prague Proposals, a set of recommendations on how to build securely and resiliently 5G

networks based on free and fair competition, transparency, and the rule of law.

We have been working to advance the principles in the Prague Proposals by encouraging other countries to endorse them. We have also signed a number of memorandums of understanding (MOUs) for research and development (R&D) in the application of 5G technology with like-minded countries, including Romania and Poland and will soon sign one with Estonia. We are also working with many other countries in the same regard.

On October 9th to be exact, the European Commission and EU member States released their own coordinated risk assessment on 5G. We were very encouraged that the risk assessment clearly identified the risk that 5G network suppliers, of them being subject to pressure and control by a third country, especially in countries without, "legislative or democratic checks and balances in place."

The EU risk assessment itself is a sign of progress in our 5G campaign, and it demonstrates that our allies and partners are recognizing the risk of untrusted vendors, but our work is far from over.

Next, the European Commission and member States will use that assessment to develop and agree upon a toolbox of security measures by the end of the year. It is vital that this toolbox address the vulnerabilities and risks that have already been identified in their assessment, including from untrusted suppliers, and that member States then implement those security measures in their own binding national measures to safeguard their networks, just as we are doing in the United States.

Thank you for the opportunity to appear today.

Chairman JOHNSON. Thank you, Mr. Strayer.

Our final witness is Jessica Rosenworcel. Ms. Rosenworcel currently serves as a Commissioner for the Federal Communications Commission. In this role, she works to foster economic growth and security, promote accessibility, and develop policies to help expand the reach of broadband to schools, libraries, hospitals, and households across the country. Prior to joining the FCC, she served as senior communications counsel for the United States Senate Committee on Commerce, Science, and Transportation. Ms. Rosenworcel.

TESTIMONY OF THE HONORABLE JESSICA ROSENWORCEL,[1] COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

Ms. ROSENWORCEL. Good morning, Chairman Johnson, Ranking Member Peters, and members of the Committee.

For the last decade, the United States has led the world in wireless technology and performance, and we have reaped the benefits. The smartphone revolution began here on our shores, and it helped secure our global dominance in the technology sector.

So now let me be blunt. That authority is being challenged. Extending this leadership into the next generation of wireless technologies known as 5G is going to be difficult. Of course, it is worth the effort because these networks are going to kickstart the next big digital transformation.

[1] The prepared statement of Ms. Rosenworcel appears in the Appendix on page 71.

However, earlier this year, the Defense Innovation Board, which is our military's premier advisory board of academic researchers and private-sector technologists, surveyed the State of 5G networks and issued a sober warning. They found that the country that owns 5G will own innovations and set the standards for the rest of the world, and that country is currently not likely to be the United States.

This is a clarion call. Other nations saw very clearly the success the United States had in the last generation of wireless technology, and they are working overtime to ensure they secure a leadership position in 5G.

We see it in deployment. Switzerland, South Korea, China, Germany, and Japan are making great strides with their 5G efforts. We see it in activity in standards bodies, like 3rd Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU), where 5G specifications are being hammered out right now.

And we see it in patents and equipment. Chinese companies own 36 percent of all 5G standard-essential patents. Here in the United States, our companies hold just 14 percent. In fact, there are no longer any United States-based manufacturers of key 5G network equipment. The truth is we are facing well-resourced challenges to our 5G leadership from every direction, and so far, we do not have a comprehensive national plan to meet this challenge. We need one, and here are four ideas it should include.

First, if we want to lead in 5G, we have to secure the 5G supply chain. To this end, at the FCC, we have a rulemaking to ensure that our universal service fund (USF), which provides billions annually to help support broadband in rural America, will not be used to purchase insecure network equipment. This rulemaking has inexplicably stalled at the agency for the last year and a half, but now perhaps since you announced this hearing, we have publicized we will vote on this in 3 short weeks.

Second, we need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far. We need to start researching how we can build networks that can withstand connection to equipment vulnerabilities around the world.

One way to do this is to invest in virtualizing radio access networks Open Radio Access Network (O–RAN). If we can unlock the RAN and diversify the equipment in this part of our networks, we can increase security and push the market for equipment to where the United States is strongest in software and semiconductors.

Third, we need smarter spectrum policy. To date, the FCC has aggressively focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. This is a mistake. The rest of the world does not have this singular focus on high-band spectrum and with good reason. These airwaves have substantial capacity, but the signals do not travel far. That means commercializing them in all but our most urban locations is impossible. This is not good for rural America, and it could mean with 5G, we deepen the digital divide.

So the FCC needs to change course and make it a priority to auction mid-band spectrum, which is better suited to extend the promise of 5G service to everyone everywhere.

Fourth and finally, with 5G, we are moving to a world with billions of connected devices around us in the Internet of Things. We need to adjust our policies now to plan for this future.

Here is what that could look like. Every device that emits radio-frequency at some point passes through the FCC, and if you want proof, just pull out your smartphone or look at the back of your computer or television. You will see an identification number from the FCC. It is a stamp of approval. It means the device complies with FCC interference rules and policy objectives before it is marketed or imported in the United States. The FCC needs to revisit this process and use it to explore how we can encourage device manufacturers to build security into all new products.

And to do this, we could build on the National Institutes of Standards and Technology's (NIST) draft set of security recommendations for devices in the Internet of Things, but the most important thing we need to do is get started right now.

Chairman Johnson, Ranking Member Peters, and Members of the Committee, thank you for having me here today. I look forward to answering any questions you might have.

Chairman JOHNSON. Thank you, Ms. Rosenworcel.

I really appreciate the attendance of my colleagues here, and so out of respect for their time, I will delay my questioning and turn it over to Senator Peters.

Senator PETERS. Thank you, Mr. Chairman.

On Monday, Chairman Pai of the FCC presented a plan to address the supply chain risk in our networks. This includes a proposal known as "rip and replace" that would require carriers receiving support from the universal service fund to remove existing equipment and services deemed to be of national security risk from their networks and provide financial assistance to those companies that do that.

To Commissioner Rosenworcel, is there a comprehensive database or map where Huawei and ZTE equipment has been deployed in the United States?

Ms. ROSENWORCEL. Thank you, Senator Peters, for the question.

No, there is not right now. It is my hope that with this proceeding, we can develop one. We know we need to. Much of this equipment lies next to military bases in this country. It is insecure, and we need to move it out.

Senator PETERS. So who should be developing it, and what process would that look like?

Ms. ROSENWORCEL. I think we have to start with our Notice of Proposed Rulemaking and seek comment on where this equipment lies, how much of it is out there, and at what point in its useful network life cycle it is at, because we have to understand where it is before we decide what dollars we make available to help rip and replace it.

Senator PETERS. Mr. Krebs, and then I would like the rest of the panel to comment. If we do pursue this rip and replace approach, should it apply to all equipment, without exception?

Mr. KREBS. Can you clarify? Do you mean just within rural deployments, or do you mean Huawei and——

Senator PETERS. Huawei and ZTE.

Mr. KREBS [continuing]. Globally Information and Communications Technology (ICT) across the United States and every environment? I would hesitate to go that far. I think we need to look and understand where the risk truly is and focus our efforts there, particularly if we are talking Federal resources getting into play here, but again, focus on where the risk lies and focus our efforts there.

Senator PETERS. If we could just go down the panel, if we could, please.

Ms. RINALDO. Yes. I would just echo that. NTIA works closely with DHS in their Information and Communications Technology and Services Supply Chain Risk Assessment Task Force. So these are the types of the conversations that we are having, understanding that there is only a certain amount of money available. We want to make sure that we are being smart with that deployment.

Mr. STRAYER. I think it is important to recognize, Senator, we are talking about existing 4G networks that have this unsecure equipment. We move to 5G; the risk profile changes dramatically and really increasing the cyberattack surface area. So more parts will become critical, as there is the smart computing moving out to the edge more. So I think a vast new array of technology that is not considered critical will become so in the 5G network.

Ms. ROSENWORCEL. I largely agree with my colleagues, but I would say the primary focus right now should be the $4.5 billion a year that the universal service fund contributes to rural carriers across this country to deploy broadband.

Senator PETERS. Well, that actually is a question. How should the cost and impacts of rolling this out in rural communities be factored into the risk-based decisions that I think I have heard everyone say? How would you do that?

Ms. ROSENWORCEL. I think we have to start with this rulemaking and make some assessments about it and work with this Committee to identify what our priorities should be, but I think that we can all agree that the goal is to take this equipment out of our networks and to make sure it is no longer there as we head to 5G.

Senator PETERS. Anybody else on rural?

Yes, Mr. Krebs.

Mr. KREBS. I think this is the right course of the conversation. I think what we also need to focus on are what are the economic realities of a flash cut of pulling this equipment out today from 4G, what as you mentioned, what Commissioner Rosenworcel mentioned, what is the life cycle. How are they going to age this stuff out if it is going to happen over the next 12, 18, or 24 months? And we can contain or manage the risk. Maybe we let it go naturally through the process.

Just yesterday in Denver, Colorado, the U.S. Chamber of Commerce hosted an event, a Rural Engagement Initiative, that brought regional rural providers together with representatives from everyone that you see up here. In fact, some of the folks in the room were there.

One of the outcomes that came out of that engagement was on the provider side, the telecommunications provider side, to help develop what a playbook looks like for flash cut and what the associated costs might be.

So, again, I think we are on the right track. I think a Request for Proposal (RFP) or a radio frequency interference (RFI) process is likely a good way to elicit information as well.

Senator PETERS. I think you raise an important point. We are going to have a gap if there is a ban on Huawei and ZTE. How would the Administration deal with the costs associated with that? Any idea?

Mr. KREBS. I think that is the right conversation to have between the Administration and Congress on what the appropriate cost sharing or the cost burden between Federal Government and the private sector and, in some cases, State and local authorities of who is ultimately responsible.

Again, we are not talking about pulling all this stuff out tomorrow. There is a reasonable plan likely that would allow for transitioning out over the next year and a half to 2 years.

Senator PETERS. Commissioner?

Ms. ROSENWORCEL. I agree with that. The estimated costs of removal right now are between $700 million to $1 billion, but the one good fact we have is we have a template for this.

Congress in 2012 asked the FCC to help with the relocation of broadcasters in the 600 megahertz band and set aside funds for us to do just that. We should borrow the template we used for that repurposing of equipment. It involves audits, site visits, certification of where equipment is and is not, because I think it has worked well, and I think it could serve us well in this environment too.

Senator PETERS. If the FCC proposal is approved, American companies and citizens will still have to transmit and connect with networks abroad, as I think you mentioned, Commissioner, in your opening comments, that use Huawei and ZTE equipment.

My question is for you, Mr. Strayer. Does the FCC's most recent action protect U.S. equipment and networks from vulnerabilities abroad, or do you share some of the concerns that we have heard from the Commissioner?

Mr. STRAYER. I think the primary concern abroad will be that as we are increasingly interconnected, if there is ability to disrupt critical services abroad, that will quickly have an impact in the United States. So they will have follow-on impacts almost immediately in the United States from having unsecure networks if they are compromised by having untrusted vendors.

Senator PETERS. Commissioner, can you expand on your comments that you made in your opening?

Ms. ROSENWORCEL. Yes. Listen, I think my colleague here, Rob, has done incredible work going around the world and pressing our diplomatic case for removing this equipment from other nations' networks and not investing in it for 5G, but the truth is we are going to need other plans on the table too.

That is why I mentioned virtualization of the Radio Access Network. We are going to have to start thinking about technologies

that allow us to be secure in a world when we have to connect to insecure networks.

Senator PETERS. Great. Thank you.

Chairman JOHNSON. Thank you, Senator Peters.

A real quick comment on the rip and replace. Ms. Rosenworcel, you are quoting figures that I also heard from some of the vendors. I would just suggest, as we are trying to undertake that study to talk to those alternate vendors because they probably bid on this, and they probably know exactly where that equipment exists, not only here, but also in Europe, which would be a little bit more expensive.

But, again, the 700-to $1 billion when you are talking about a significant national security threat, that sounds like probably a pretty manageable cost that we ought to seriously consider. But, again, I would really suggest that government agencies go to those alternate vendors who probably quoted on this.

Next, Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Well, thank you, Mr. Chair, and thank you to you and Ranking Member Peters for holding this hearing.

Thank you to our witnesses for taking the time to testify and help educate us all on this topic.

As a Red Sox fan, I will give a begrudging congratulations to the Nats but acknowledge that we waited 86 years. The Nats waited 95. So we feel your joy this morning.

I wanted to start with Ambassador Strayer on this topic of our diplomatic efforts. I recently traveled to India and met with India's cyber coordinator. During this meeting, we learned that while India is very concerned about privacy and about some of the warnings that we have been trying to impart about Huawei, the country is seriously considering using Huawei's infrastructure for India's 5G rollout.

They talked about, "Well, we are just doing a pilot. They could come and do the pilot." I said, "How long would the pilot last?" They said, "A year." That is a long time.

Moreover, many of our European allies who are ordinarily concerned with transparency and data privacy are still considering incorporating Huawei devices into their 5G infrastructure, even though alternatives are available from EU-based companies.

So, Ambassador, can you tell us what else we should be doing as kind of a follow up to the Commissioner's points? What else should we be doing to convince allies, partners, and other nations to move away from Huawei and ZTE infrastructure? What resources do you need to succeed in this mission?

Mr. STRAYER. Thanks for that very insightful question. I am glad you were able to raise that with the Indians.

We were doing a similar dialogue with them just a few weeks ago. There is no doubt that the cheap price point for some of the Huawei and ZTE equipment has allowed them to get into, if you will, the legacy networks. As they move to 5G, many of the telecom operators argued that it is going to be cost prohibitive for them to use a more secure vendor.

There is analysis that shows that myth busting a lot of these arguments that the telecom operators are throwing out there.

First of all, they are not going to fall behind technologically if they go with one of the EU vendors or Samsung. In fact, Reliance Jio, one of the largest telecom operators in India, is using almost exclusively Samsung at this point, and, of course, we in the United States are using those providers. There is no way you fall behind technologically.

There is also no real concern or should not be a serious concern about cost. Any technology in the networks that is pre-2016 has to be replaced anyway. So you are only looking at the last couple years of deployment, and there are ways to make that be replaced on a normal life cycle.

There are other concerns that these countries have that include kind of coercive measures that the Chinese can use against them if they were to not allow their national chain to participate.

Senator HASSAN. So, given that, let us just follow up for a minute. I understand all those arguments. They are some of the same arguments I have been making to countries like India, along with you, but it does not seem that our partners are listening. So what else should we be doing, or what additional resources do you need?

Mr. STRAYER. So, on that front, I think we are getting the understanding. Almost every country now says they will prohibit the untrusted vendors from the core of their network. So that begs the question why allow them in the edge, and what is the value of the data that is at the edge that they are going to be willing to give up?

As far as additional resources, we are already thinking about how we have initiated programs to help improve connectivity, and that is trusted connectivity in developing countries. So we already have some of that moving in the right direction as far as resources to help develop trusted networks.

It would be helpful as you as Senators or delegations to these countries around the world that you talk to their parliaments. This is not just a technical discussion. Some would want this to be resident in some kind of technical telecom discussion. This is really about our fundamental values——

Senator HASSAN. Yes.

Mr. STRAYER [continuing]. And about geopolitical threats because it is inherently impossible to test your way into security when it comes to telecom technology, and that is because you can always insert a back door in the tens of millions of lines of code.

So if you as members are willing to go out there and talk to parliamentary colleagues around the world, I think that would help us a tremendous amount to make sure that they are invested in the political process. This, at the end of the day, has to be a political process, not just a bureaucratic process.

Senator HASSAN. OK. Then to follow up on that point, to all of the witnesses—and very quickly, if you can—5G is still taking shape. Technical standards that guide how 5G will ultimately work are being actively developed in international standards-setting forums, and you have all referenced that.

It is vital that the United States drives this conversation, and that China is not allowed to dominate the future of 5G to the detriment of the United States and our allies.

So from each of you, how are your organizations coordinating engagements in the international standards bodies in order to counteract China's influence? Because China is being really aggressive on this.

I will start with Mr. Krebs.

Mr. KREBS. So we directly coordinate both through the NSC process and also as an operational agency to agency to ensure that when we deploy to the 3GPP or other standards bodies that we have consistent direction and priorities working with our industry partners.

Senator HASSAN. OK. Ms. Rinaldo, anything to add?

Ms. RINALDO. Yes. NTIA actually participates at 3GPP on public safety issues as well as FirstNet, which resides under us. So we are there on the floor talking to people.

Senator HASSAN. OK. Go on.

Mr. STRAYER. The international conferences on worldwide spectrum policy is taking place right now in Sharm el-Sheikh, Egypt. We have a delegation of 120 people from the private sector and from government there. Chairman Pai is there. We have an ambassador from the State Department there leading that. So we are leading these international bodies.

I think that this word about standard essential patents, you can carve that a lot of ways. Certainly, the Chinese propaganda has been to assert that they are leading, but there is a report out today that says Intel and Qualcomm have the most valuable of what are likely to be standard essential patents.

So it is a competitive space, and we need to be vigilant, but I think we are in a very good place for the future.

Senator HASSAN. Go ahead.

Ms. ROSENWORCEL. I agree with you that we need to assess if all this interagency coordination is really working, and the best way to do it is after the World Radio Conference, which is taking place right now in Egypt, to come back and assess what our experience has been with the 193 nations and how successful we have been at moving our spectrum policies forward.

Senator HASSAN. Thank you.

I have a couple other questions. Mr. Krebs, briefly, I want to invite you to come to New Hampshire and work with some of my local and county folks on the issue of ransomware because I think we need to have increasingly better partnerships on that. So can you commit to helping us with that?

Mr. KREBS. Absolutely. This is a huge area of focus for us right now, not just on normal State and locals, but also as we think about elections and voter registration databases, a big initiative area for us right now.

Senator HASSAN. OK. Thank you.

I am running out of time, but I am going to ask—if I come back and we are still having the hearing, I want to follow up with Commissioner Rosenworcel on the issue of the FCC auction of mid-band spectrum and how important that is going to be in terms of the rural-urban digital divide. So I hope to follow up with you on that.

Thanks.
Senator JOHNSON. Quick answer, it is important.
Senator Romney.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY. Thank you, Mr. Chairman, and thank you to each of you who are working in this very vital area.

In a lot of respects, it is sad that we are having to hold this hearing. It is extraordinary that China has been able to take such a substantial lead in an area that is not only important for us economically but vital to national security, and my prediction is that we will be repeating this picture again and again in various other areas that are important economically and with regards to our national security.

This is the first example of what is going to happen again and again, and I guess I would like to address my question to all of you or whoever would like to respond to it as to how it is, if you will, free market economies were unsuccessful in establishing our own lead with regards to 5G—how is it that Chinese companies were able to get so far ahead of us on the track that we are trying to chase them and catch up to them?

I would note that China has a very clear strategy as to where they want to be in 5G but also economically, geopolitically, militarily, and we as a nation do not have a strategy. We respond on an ad hoc basis. When we see them ahead on the track, we say, oh, we have to do something about that, but always chasing your competitor is not a successful strategy.

And not only do we not have a strategy to deal economically with a player that does not play by the rules, we do not even have a process under way or much focus under way nationally to describe how we are going to compete with a nation that continues to break the rules, how we and the West will do so.

I only think this can be done on a collaborative basis with ourselves and other free nations, and so we would keep Ambassador Strayer from having to run around, country by country, begging people, "Oh, please do not do what is in your best economic interest. Hold on because we have something better coming along." This just does not make sense as a strategy for our Nation.

I will go back to my question and say how is it we got so far behind on 5G with such extraordinary companies, in many cases, not in the United States, but companies in South Korea, companies in the EU, that participate in this area? How did China get such a big lead? Why did we let them get so far ahead?

Mr. STRAYER. If I may start, Senator. I would say at the front end that we do have, roughly, a general strategic guidance from our National Cyber Strategy, and we are taking on China across a range of areas, especially holding them accountable for their inability or their reluctance to implement the rules-based international order that they agreed to when we let them accede to the World Trade Organization (WTO).

And I think it is also important in 5G to recognize that Cisco, Intel, Qualcomm are world leaders in the technology. What we do not produce is the hardware that forms this Radio Access Network, and we are quickly moving in that direction and thinking about

how we can virtualize more functions and moving to the area where we will be really strong, which is in software with more generic hardware.

I think that is how we have a general mission. We are talking to our partners and allies about trusted technologies, emerging technology of the future to set the right rules of the road, but fundamentally, these Chinese companies are not competing in any type of capital system of free and fair markets. They are being subsidized substantially. So we need to think about targeted R&D and efforts to work with our allies to see how we can each play to the best of our strengths.

Senator ROMNEY. Thank you.

Mr. KREBS. As Ambassador Strayer mentioned, I think we are kind of in a blip. The piece that the Chinese own the most is the Radio Access Network. I think given some of the comments and particularly Commissioner Rosenworcel mentioned about focusing on virtualization and Open Radio Access Networks, I think if we were to hold this hearing in a year to 18 months to 24 months, a completely different conversation about the options, trusted options available in the marketplace.

So what we have to do is make sure that we sync up the timelines, particularly on an international basis. I encourage everyone, if you have not already, go look at the Huawei Oversight Board Report that the United Kingdom (UK) issued earlier this year. It is a pretty damning document in terms of an evaluation of the security quality of Huawei products, and this is from a country that has been assessing technically, from a cybersecurity perspective, the quality of Huawei products now for 10 years.

First, they said not much improvement over that 10-year period. Moreover, the transformation plan that Huawei has issued indicates that, by their own admission, Huawei's own public estimates are that this transformation to bring Huawei's equipment to a commercially reasonable cybersecurity posture will take 3 to 5 years.

This is sufficient evidence for us, as Rob goes around the world and talks about "Do not make a bad decision now. You will be paying for it for the next 10 years." This is the sort of the evidence we need to say, "Hold on. Let us work, and let us incentivize this alternative trusted vendor base to emerge, to flourish," and I think this is the opportunity in front of us. We have to put a lot more effort in, whether it is DOD in their RFP that they have recently issued or they will be issuing on experimentation to encourage these companies to come forward.

There is great opportunity in front of us. Again, my hope is that a year from now, a little bit more than that, a different conversation.

Senator ROMNEY. Please.

Ms. RINALDO. Just to echo those comments, at the Department of Commerce, we really look to answer that question. If not them, then who? And we do see the American companies, the software vendors that are going to fill that void, with software-defined networks.

You also often hear that the Chinese sent swarms of people to the standards body, and they vote en block. Whereas, we go, work

with our partners, work with industry, but that is where you are going to get the best product.

I think as we discuss what is the answer to our success, how do we win the race to 5G, it is not being more like them. It is doubling down on us. So that is what we are focusing on and collaborating together on.

Senator ROMNEY. Thank you.

Ms. ROSENWORCEL. Senator, I think you are right, and I think the evidence is around for all of us to see.

In today's *Wall Street Journal*, it mentions how China will have 130,000 cell sites equipped for 5G by the end of the year. South Korea will have 75,000, and the United States will have 10,000. The truth is we have rested on our 4G laurels, and that is not a good place to sit. If I had to choose one thing that we should change right now, we need a spectrum strategy that makes sure 5G service gets to everyone all across the country.

We have doubled down in the United States on auctioning high-band spectrum, which propagates between one corner of this room and the other. We will never make that an economic way to deploy 5G everywhere, and it will reduce our power and our scale for equipment, devices, and innovation.

Senator ROMNEY. Thank you.

Chairman JOHNSON. Just real quick, as long as we are on the topic, I do want to throw out the question. Does it make sense for the Federal Trade Commission (FTC) to be suing Qualcomm under antitrust? Does that lawsuit continue to make sense? Ms. Rosenworcel

Ms. ROSENWORCEL. That is outside of my jurisdiction, but I will acknowledge that——

Chairman JOHNSON. It is close—FCC, FTC.

Ms. ROSENWORCEL. Yes, I know. It is just one letter, right?

I will acknowledge that the United States has really powerful operators when it comes to software and semiconductors, and we should figure out how to use that as we forge our way into the future.

Chairman JOHNSON. Anybody else want to comment on that? It has me scratching my head. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Mr. Chairman, thank you. Thank you all for the work that you are doing on this. It is exceptionally important.

I have a lot of folks that will catch me about the access to data that Facebook or Google or different Internet providers will have—or Microsoft will have, and they will say they have access to a lot of data. I will typically smile at them and say no one has more access to your data than your cell phone does because they have all of those plus a whole lot more, and it is remarkable to me how little focus there has been on the security around everything that goes through your cell phone.

And for folks in rural Oklahoma, they would tell you that many of their irrigation systems are connected to their cell phones. Control systems for valves are connected to cell phones. So whether it is energy, agriculture, or manufacturing, it all goes through this cell network. So thank you for your focus on the 5G on the security

because we cannot get this wrong, because every bit of our data and every bit of our manufacturing and our systems and our inventions all go through this system. So I appreciate you doing this.

Let me come back to the spectrum conversation. Why is not there a conversation on the mid-band right now?

Ms. ROSENWORCEL. Well, there is a conversation, Senator, on mid-band spectrum right now.

My primary concern is that the FCC during this Administration has chosen to put all of its earlier efforts on high-band. We have auctioned the 24 gigahertz band, the 28 gigahertz band. By the end of this year, we will have the 37 gigahertz band, the 39 gigahertz band, and the 47 gigahertz band.

Senator LANKFORD. So why not the mid-range?

Ms. ROSENWORCEL. You and I have the same question. I think we should have prioritized the 3.5 gigahertz band and done it 2 years ago because those are the airwaves that are going to help us reach rural America and urban America.

We are making a mistake, and the rest of the world is not auctioning high-band spectrum. There are 16 nations right now that have already brought mid-band spectrum to market. That is where the bulk of the economy is going for wireless, for 5G, and the United States is behind.

Senator LANKFORD. So let me switch topics on that, because that is helpful. We will follow up on it. Let me switch topics on the hardware side of the manufacturing in this system.

You have all mentioned that one of the issues we have is not necessarily the software. We have a lot of software that is currently very innovative. It is the hardware manufacturing side of that.

What is missing in the hardware side of it is that we have just outsourced the hardware for so long to China and to other places that we just do not have the locations. Is it a raw material issue? It is certainly not a creativity nor capital issue. We have that in the United States. So what is the gap on the manufacturing side?

Ms. RINALDO. On the manufacturing side, I have heard—that 40 percent of the makeup of the network is actually American manufacturing companies. It is the RAN that does not have a U.S. hardware manufacturer.

Senator LANKFORD. Correct. That is the part I am talking about.

Ms. RINALDO. Right. I think when we talk about software defined networks to innovate around that problem, that is where we are going to inject the innovation to create the networks of the future. So that is what we are focusing on now, and we believe there is beta testing as we speak, and that it could be a reality in as early as 18 months.

Senator LANKFORD. So you are saying the radio access is not as needed if we can have a software workaround?

Ms. RINALDO. Correct.

Mr. STRAYER. Senator, I would just point out that the reason that the old Bell Labs became Lucent and it got bought by Alcatel, a French company, that got bought out by Nokia—so there is still research going on in America in this area. It is just that it is owned at the headquarters level in Europe, and there is going to be new manufacturing by Ericsson in Florida. There is Samsung fabrica-

tion of chips going on in Austin, Texas. They put $17 billion into it. So there is going to be manufacturing.

The long-term solution, I think, is the lines of the acting administrator's point, but we do see manufacturing here. And there is obviously competition coming from China that is massively subsidized. So that is really where the market is failing is in subsidization.

Senator LANKFORD. Mr. Krebs, this is something you track all the time on the supply chain issues. As you know extremely well, if we have one bad link with data, that is the spot to get a chance to infiltrate unlimited amounts of data. When you start looking at supply chain issues, where do you see the gap? Where do you see the engagement? What is it that the U.S. Congress and the U.S. Government needs to be involved in, or what do we need to do less of to allow that market to be able to grow?

Mr. KREBS. I think supply chain is an emerging area of focus for certainly my agency but the rest of the Administration. It is much like cybersecurity. It is about identifying where the risk lies, managing that risk appropriately, and putting your attention where the gaps are.

This time last year or a little bit earlier, we established an Information and Communications Technology Supply Chain Risk Management Task Force. Again, all the agencies here are represented on that task force, 20 Federal agencies, 20 tech companies, and 20 coms companies, 4 different work streams.

One, first and foremost, is, What does information sharing look like on supply chain risks? Second, what is a threat profile or the categories of threats we need to be concerned about? Third is, How do we develop trusted qualified bidders list, kind of white listing? And, last, how do we incentivize purchasing from original equipment manufacturers and trusted resellers to eliminate the counterfeit problem?

This is an incredibly important area of work because it gives everyone, whether you are super-sophisticated, highly leveraged and invested in supply chain issues, or down to just your average, somewhere, subcontractor in a supply chain conversation. It gives them a common operating language or a common framework by which to assess.

One of the big things that I think came out of this conversation is when we talk about information sharing, when we talk about sharing threats of companies that may be of concern, there are examples—the National Regulatory Framework 10, Code of Federal Regulations (CFR) Part 21, has a reporting of defects and noncompliance. If you come across something in supply chain, you have to report it.

There is no similar standard for other high-risk areas of infrastructure.

Senator LANKFORD. Is that a gap in the law? Is that a gap in regulatory?

Mr. KREBS. I think, at this point, it is probably both, but I would focus on how do you have a company that comes across an issue with an untrusted vendor. They have significant civil litigation risk for publicly outing that company. How do we give them the appropriate information-sharing protections that they can make a report

into whether it is government or other industry partners, get away from antitrust issues, anticompetitive issues? This is an area that I think we think needs more attention.

Senator LANKFORD. Let me bring up two quick things on this. One is, as we are going through supply chain conversation, we need to deal with the raw materials and rare earth minerals. That has been a weak area for us as a Nation. We have been complacent to allow rare earth minerals to come from China and to say, well, they are going to manufacture, they are going to mine, they are going to handle all that, but we have environmental issues, and so we are not going to do rare earth minerals.

We can do it cleaner and better than anywhere else in the world, and we should lean in on that one. That is near where we need to identify.

Ms. Rosenworcel, one of the areas that is not related to this, but every time I see anyone from the FCC, I bring up one issue with them, and that is prison cell phone jamming. We are not going to talk about it, but I just want to be able to bring it up and to say it is allowed in Federal prisons. It is not allowed in State prisons, and that is an area, a gap in the law, that we need to address. But we need FCC's engagement on working through standards for when that jamming device is actually done and tested. They will want to test against a group of standards. FCC is the one who has to establish that.

We have major problems with contraband cell phones across the entire Country in prisons, and we need the FCC to engage in this area.

I know it is a surprise question to you. I am not going to ask you to respond to it, but I am not going to also miss the opportunity to say we need that.

Thank you.

Chairman JOHNSON. Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. I remember, Senator Lankford, being down in Guatemala, maybe with Senator Johnson. We were meeting with the president of Guatemala, and I said to him, "You know, we have been visiting some of the prisons. You know, there is technology that you have, Mr. President. Your prison guards are allowing cell phones to be used by criminals in the prisons and conduct their criminal business," and he said, "Really?"

I said, "Yes. There is technology that can jam those," and he said, "Really?"

I said, "Yes. You have it in your prisons." He said, "Really?"

I said, "Yes. And you do not use it." He said, "Really?"

I said, Yes. You know who is responsible for making sure that this stuff is there and has used it is your interior minister. He is sitting right here, and he is not making sure that is being done," and he said, "Really?"

I said, "Yes."

Six months later, they were both in prison, and I hope they are using their cell phones badly. But I think it is an important point and not just for the United States.

Ms. Rosenworcel, I love your name. Have you always been a Rosenworcel?

Ms. ROSENWORCEL. I have.

Senator CARPER. OK, good. I would stick with that one. [Laughter.]

You ran through four ideas to help secure U.S. leadership on 5G. Just say those again quickly, and I am going to ask your colleagues to respond to them and just say whether they think you are making sense or not.

Ms. ROSENWORCEL. First, secure the supply chain. Second, we need to think beyond supply chain and look to virtualization of Radio Access Networks. Third, we have to be smarter about the spectrum that we auction and auction more mid-band spectrum, and fourth, we have to come up with policies to secure the billions of devices in the Internet of Things.

Senator CARPER. Mr. Strayer, nice to see you.

Mr. STRAYER. Great to see you, Senator.

Senator CARPER. In fact, do I call you "Mr. Secretary" now?

Mr. STRAYER. No. I guess everyone has titles in this town, but I will stick with being in a town with the Washington Nats as the world champions.

Senator CARPER. Very good. That is great.

Mr. STRAYER. If I can respond just briefly.

Senator CARPER. My favorite baseball team is the Detroit Tigers. We had the worst record in baseball, but three of their best former pitchers—four actually, Porcello, Red Sox. Gary and I are both Tigers fans. We traded off Verlander. We traded off Max Scherzer, and we traded off Sanchez. Someday we will be good again. It will not be anytime soon.

Mr. KREBS. Thank you for those two pictures.

Mr. STRAYER. The farm team.

Senator CARPER. We have really good arms in AA and AAA.

Mr. STRAYER. Right.

If I may, I completely agree that we need to work on the supply chain. I do not know if I mentioned it yet today, but President Trump signed an Executive Order on May 15th of this year—he declared a national emergency to supply, to protect our domestic communications technology, and that will soon be followed by binding regulations later this year.

I think, 100 percent agree with the idea that virtualization of the functions of the Radio Access Network will be very important to allow the breakup of the proprietary lock-in that many of the current Radio Access Network providers have today, and that will also reduce cost on capital expenditure as well as operational cost for providers. So it can be very competitive with regard to some of the current providers, such as those in China, if we move toward more virtualization.

On the mid-band point, I think it is worth noting, first of all, that getting to rural areas, under the T-Mobile/Sprint merger, in the next 3 years, they are required to cover 97 percent of the U.S. population and in 6 years to cover 99 percent of the U.S. population.

Now, the FCC, I understand, is going to proceed with proceeding on the 3.5 gigahertz mid-band spectrum next summer. They had to

prioritize some of the millimeter-wave, but I think we should not denigrate the importance of millimeter-wave that is going to be so important to manufacturing and other use cases that are going to require the most maximal amount of throughput, which is only available through millimeter-wave. That is the kind of beauty of that technology is that it does not go as far, but it has the greatest amount of data transmission available.

Of course, Chairman Pai has said by the end of this fall, we are going to have a plan to move forward on the C-band, which is also mid-band, and I understand 2.5 gigahertz will follow probably in the next year after that.

So we certainly need to keep moving forward with this, but we have, I think, sufficient plans to ensure that we have mid-band available in the blend of low-band, mid-band, and high-band spectrum that we need.

Senator CARPER. Thank you.

Ms. Rinaldo, I am going to ask you to answer briefly. Do you find any of her four ideas favorable with you? Which ones? Yes? No?

Ms. RINALDO. Yes. Thank you.

So, at NTIA, we are the Federal regulator for government-held spectrum. We also represent the Administration in FCC proceedings, and the Administration believes that you need low-, mid-, and high-band in order to be most effective with the 5G deployment.

The Making Opportunities for Broadband Investment and Limiting Excessive and Needless Obstacles to Wireless Act (MOBILE NOW ACT) tasked NTIA to look at the 3.1 to 3.5 GHz Lands, and that review is currently under-way. We have a report due to Congress next year.

As Deputy Assistant Secretary Strayer mentioned, there is an auction next June on Citizens Broadband Radio Service Device (CBRS), which is mid-band, and then there is one this December on high-band. So we are hitting those important notes.

Also Commissioners Rosenworcel mentioned supply chain. The Executive Order gives the Secretary of Commerce the emergency authorities to make determination against transactions that could be concerned with untrusted vendors in our network. So we are currently putting together the regulations on that as well.

And we are all in agreement that software-defined networks and Open RANs are going to be a game changer of for us.

Senator CARPER. Alright. Thanks.

Do you agree with anything that she said? Ms. Rosenworcel, that is.

Mr. KREBS. I agree with everything she said. Supply chain security, a huge area focus for CISA going forward as well as securing the Internet of Things.

Senator CARPER. Alright. Thanks.

All of us could tell you stories about how some of our students, our schools, our businesses are struggling in rural parts of our States. We can all tell you stories for lack of access to the Internet.

I would ask of you, Ms. Rosenworcel, if you would, having said that, what is the commission—you talked about this a little bit already, but what is the commission doing to ensure that the Internet is accessible to all communities and that 5G deployment is not

another technological advancement that leaves the rural communities even further behind?

Ms. ROSENWORCEL. Yes. Thank you, Senator. Such an important question.

We need to do more. We have a digital divide in this country. It is real. We have 12 million kids who cannot even do their homework because they do not have Internet access. They are in every State.

Senator CARPER. Some of them are not complaining, but they need to be doing their homework.

Ms. ROSENWORCEL. We want them to be able to access the Internet and do their school work, and it is just a window into this challenge we have. We have to fix it.

I think we would start with better mapping. I know that Senator Peters has a bill on just this subject. Right now, FCC maps wildly overstate where broadband is and is not in this country. Go to every rural community. They will tell you. They do not have service. Yet if you look at the FCC map, we found one subscriber in a census block, and we decided that it is available throughout. That is wrong. We are never going to know where to devote our scarce Federal resources if we do not first get our maps right.

Senator CARPER. Let me just interrupt you. Aside from grants, what other support can government agencies provide to help advance Internet access?

Ms. ROSENWORCEL. I think that by refocusing now on mid-band spectrum, we could make a meaningful difference in the deployment of 5G. It propagates further and requires fewer towers. It is more economic to deploy in rural communities, and if we want rural America to see 5G, I think we have to focus on that sooner rather than later.

Senator CARPER. Alright. Thanks.

Mr. Chairman, Albert Einstein's wife as much—he was married to a brilliant woman, and she was once asked if she understood her husband's theory of relativity. And she responded, famously. She said, "I understand the words but not the sentences."

I just want to say that a hearing like this is helpful to me in not just understanding the words but some of the sentences too. So thank you all.

Chairman JOHNSON. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Well, Chairman, thank you for having this hearing. I apologize. I had another commitment earlier, so I did not get to hear all the testimony. But I did have a chance to review it.

To me, this is ultimately about our competitiveness as a Country, and we have kind of all the ingredients for a major problem here. One is the importance of 5G. The other is a China that I would say has become almost a techno-nationalist country, where they use State power, and often a disregard for international trade rules. This includes subsidies, but it also includes tech transfer. And often it is driving market-oriented companies out of business, and at the same time, we have a loss of production here of 5G hardware.

You talked a lot about the supply chain this afternoon or this morning, and I think that is part of the issue here.

In terms of being a driver for 21st Century competiveness, 5G just seems to me is very worrisome.

By the way, we started an Artificial Intelligence (AI) Caucus here in the Congress. We are trying to avoid getting sort of a decade behind on artificial intelligence. It is, in a sense, what I think we have on 5G. So this hearing is really timely and really important.

Commissioner, I was just listening to some of your responses, and by the way, I totally agree with you on the maps. It concerns me because, in rural Ohio, we have some areas that under the FCC map are said to have broadband capability, and they do not, certainly not for the school children but also not for a lot of our small businesses that are eager to be able to expand in some of our rural areas, but are being told it is going to be a long time and a big expense to get the ability to have fast Internet. So they tend to go to the urban areas; therefore, Columbus is expanding substantially but not southeast Ohio.

On the issue of Chinese technology being at the center of the 5G future, I think we cannot concede that. We have to figure out how to deal with that.

There are some non-Chinese 5G hardware providers, I am told, but there is no provider of that hardware in the United States; is that correct?

Ms. ROSENWORCEL. That is correct.

Senator PORTMAN. What policies do you believe we should adopt to promote the reshoring of this production, and do you believe the United States can rely on some of these non-Chinese suppliers as an alternative?

Ms. ROSENWORCEL. Thank you for the question.

First, I am confident that we are going to figure a way to make sure that the United States succeeds, but here is some important data points. At the turn of the millennium, there were 13 big network equipment providers around the world. By the time the 4G revolution started, there were seven. Now we have three or four, and I think we have to be honest about the fact that we are allowing consolidation to take place among our largest wireless providers. And by doing that, we are reducing the number of providers that equipment manufacturers can sell to. It gets harder and harder to get into the business under those circumstances. That is a problem.

I think our way out is to instead focus on where we are best, which involves software, and so what we need to do now is what you have heard from some of my colleagues—and it is in my testimony—is we have to look at the Radio Access Network and identify how we can introduce virtualization there. That would mean using off-the-shelf hardware, but its intelligence would come from United States sources and software. I think that is where we need to focus our energies, and I would like to see the FCC develop some testbeds and policies to encourage that to happen.

Senator PORTMAN. Can that be done with the current consolidation, or are you saying that these supply chains are necessarily limited because of the fewer buyers, customers?

Ms. ROSENWORCEL. I think we have harmed ourselves with the current state of consolidation. It is hard to ask new entrants to get into a marketplace where there are a very small number of potential purchasers.

But under these circumstances, I think what we have to do now is go to what we do best, and that is software.

Senator PORTMAN. Focus on software. OK.

Let me touch quickly on standards. This is a topic that may or may not have come up here today. Probably not because it may seem a little esoteric, but I have raised this issue at the Belt and Road hearings we have had at the Senate Foreign Relations Committee as well because I think it relates directly to what is really happening out there on the international front.

China has increased their membership in these international standard-setting bodies substantially and take it very seriously. We do not. It does not mean that China is going to hijack all these international standard-setting bodies, but it does mean that our interests are not going to be well represented unless we begin to put more emphasis on it.

So I do not know. Maybe, Secretary Strayer, since you use to work for this Committee and also the Senate Foreign Relations Committee, we will focus on you on this one.

In general, what do you believe the government can do to incentivize increased participation in the international standard-setting bodies, and specifically, do you believe that by making it easier to grant visas for foreign individuals to come to this country that we could have more of these standards conferences in the United States? Because we do not typically have them here anymore. And can we incentivize more of these conferences to be happening here and get more U.S. involvement?

Mr. STRAYER. Yes. Thanks for that, roughly, two-part question, and I just want to break up the standards-making bodies, between those that are dominated by governments that are multilateral, like the International Telecommunication Union, the big 5G conference that they are having to harmonize worldwide spectrum policies, occurring right now in Sharm el-Sheikh, Egypt. We have more than 120 U.S. Government officials and private-sector delegates representing us there.

So we are taking a pretty aggressive posture in all of these standards-making bodies, and I think I can let my colleagues talk a little bit about what they do, what the Commerce Department and others, how they are involved internationally in these standards-making bodies. But we are vigilant about what is going on there.

We have noticed that the Chinese have come in, in larger forces there. We think there has been a pretty successful distribution of patents coming to U.S. companies and to western companies generally. We work closely with our partners to ensure that we are having the right policy outcomes in all of those conferences.

I think it is also important that we think about how we can encourage the private sector to participate fully in standards bodies. Companies partake in standards bodies because they see a value in them. Some companies just run to market with the latest technology. So there has to be a reason that they are participating in

the standards body itself because that takes a lot of resources from their own internal research and development efforts to actually participate in these standards bodies, which can take years to bear fruit. So I think we can think about policies on that front.

Senator PORTMAN. How about the conferences? My question was in part about these visas and the fact that we are not having the conferences here in this country and that puts us at a disadvantage.

Mr. STRAYER. So we are looking at hosting a broadband conference next year, and so I think we are analyzing that.

One of the issues is that we have National Security Reviews for people coming to our conferences, and the world wants to participate in our conferences, including some countries. We have very substantial concerns about the activities of their governments and some of the officials in their governments.

Senator PORTMAN. So when was the last time we had a conference in the United States?

Mr. STRAYER. I know we had an IT conference about 20 years ago.

Senator PORTMAN. About 20 years ago?

Mr. STRAYER. And that is just one narrow sliver.

But we host all kinds of meetings all the time here on a smaller delegation level. All of Western Hemisphere comes here to Washington for the pre-meetings for the larger global——

Senator PORTMAN. Do you think it would be helpful to have some of the global conferences here on standard setting?

Mr. STRAYER. Yes. But I am not sure that it is impeded by the visa issue.

Senator PORTMAN. Is it impeded by the visa issues?

Mr. STRAYER. I do not know that it is. You are telling me this. I mean, we can look at that.

Senator PORTMAN. We are told that it is, and also, with regard to standards-setting on the private-sector side, we have an issue of American participation that we have to address. So I hope you will be doing that in your role.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Portman.

I want to go back to mid-band and just ask a question. Are there bureaucratic road blocks preventing that, or are we just moving too slow on it?

Ms. ROSENWORCEL. Thank you, Senator.

I think we are moving too slow. There are 16 other countries that have already brought mid-band spectrum to market. They are developing scale that we do not yet have.

I think that, frankly, the Administration made the easy choice, which was to focus on fairly unoccupied high-band airwaves first and push them to market through auction, but I think that is a strategic mistake.

Chairman JOHNSON. The reason I am asking, a couple months ago in a Commerce Committee hearing, we were sensing a roadblock. I had met with Chairman Pai on 24 gigahertz. I kind of raised the issue that the roadblock was no longer there, which is good.

So I am just wondering. Are there other roadblocks that people maybe are not willing to testify to at the table today? I would encourage you to let me know so we can write letters or whatever to get rid of those.

Ms. ROSENWORCEL. Our airwaves are a finite resource. We are not making more, and every one of us is using our device more often. We are using them all the time. We are demanding more from our airwaves. We are connecting more things.

So the challenge comes in how you manage the incumbents that are in those airwaves today—they are often Federal actors that NTIA oversees—and how you incentivize them to relocate and refine their operation so we can move commercial operations into the same hands.

Chairman JOHNSON. So, again, it is a difficult challenge. I just want to make sure there are not equities or bureaucratic roadblocks preventing us to overcome those challenges and get moving on this because it is a top priority.

Ms. ROSENWORCEL. Well, I think that part of the problem is our process is flawed.

Right now, the commercial actors go, and they tell us to start knocking on the doors of Federal actors that have access to spectrum. And then we go back and forth and back and forth, and it takes years.

What we should do, instead, is we should build a structural incentive into their budgets for them to be efficient with the airwaves they have, so that when they relinquish them, they see gain and not just loss from reallocation.

Chairman JOHNSON. OK. So it is a difficult problem.

Does anybody else want to weigh in on this?

Ms. RINALDO. I am happy to outline some of the work that NTIA has done over the past years on reallocating additional spectrum.

Back in August of this year, I sent a letter to all of our spectrum Federal partners asking them to assess their current needs and what could possibly be made available. We delivered a repurposing report that documented all the work that we have done.

And NTIA has also worked with the Department of Defense on dynamic spectrum sharing.

Chairman JOHNSON. No offense. I do not care to hear what you did. I am trying to go what is preventing you from moving faster. Again, I am trying to figure out what is preventing us from moving faster when this is such a top priority.

Mr. STRAYER. I just want to point out one thing that is a major impediment; that is, as you may be aware, the Sprint/T-Mobile merger will expand the better use of their massive amount of mid-band spectrum. That has been approved by the Federal Government, but it has not been approved by the lawsuit brought by the States' Attorneys General (AG). So that has been slowing that process down.

Chairman JOHNSON. So lawyers are——

Mr. STRAYER. Yes. I would just say if you look at mid-band spectrum there, that is going to cover—with mid-band, specifically by mid-band, they will cover three-quarters of the U.S. population in 3 years pursuant to enforceable terms of that merger. So I think it is important to that——

Chairman JOHNSON. I do not want to dwell on this, but I am going to encourage after this to meet with me, meet with staff. If there are roadblocks, I want to know about them so that we can utilize our oversight capacity to try and knock those things down because, again, this is a top priority.

Senator Romney was making quite a few comments about how far behind we are. I thought it was interesting in the brief, a report by the Cellular Telecommunications Industry Association, basically, in 2018 said that when looking at spectrum availability, licensing, and deployment of 5G, industry analysts concluded that China ranks highest in overall scoring for 5G readiness with South Korea and the United States and Japan not far behind.

In their April 2019 report, they said that the United States has made progress and pulled even with China.

So, again, I do not want to overstate if we are lagging. We should be ahead, but is that an accurate assessment? I mean, should we be feeling a little bit better here, or is it as dire as basically Senator Romney was pointing out?

Mr. Krebs, you are moving there. So do you want to answer that?

Mr. KREBS. I want to go back to a number of the points that the panel has made, starting with Commissioner Rosenworcel on—and that I made about this is a blip. This is just a temporal anomaly, almost. If we can unlock the Open Radio Access Network piece, the vender base in the United States, the innovation base is going to explode. Again, this is going to be a conversation we are going to think fondly back on.

Chairman JOHNSON. So you said if we can unlock, so what do we need to do to unlock that? What is the roadblock on unlocking that?

Mr. KREBS. I think there are a series of incentives that need to be put in place to provide—testbeds, for example, some of the work DOD is doing in experimentation on their bases, some of the work that I am doing with my agency at Idaho National Labs. There is a whole bunch of testing and opportunity development, but that is just a small slice of it. There are others. Federal Government contracting——

Chairman JOHNSON. Does that have to be funded by the government? Is there no private-sector incentive?

Mr. KREBS. Some of it should be funded by the Federal Government, but again, the private sector is going to surge into the market if we can make it compelling. I think the standards piece—achieving true interoperability globally is going to be critical, not just interoperability in the sense that a Huawei technical stack works together, but it is that you can start putting bits and pieces of different vendors together. That is true in interoperability.

You already think about cloud globally—Microsoft, Amazon, Google, all these cloud service providers. We dominate the hyperscale cloud market in the world.

OK. What we are talking about here with virtualized networks and O–RAN is cloud. That is all it is. It is dumb metal with software riding on top. We own that space. OK. Let us make it a compelling economic incentive for us to get in there from an O–RAN perspective.

Chairman JOHNSON. OK. So what I am asking, not at this setting, is break this down so it is understandable if there are things

that Congress can do, that this Committee can do, either targeted oversight letters to break down barriers or a piece of legislation that will incentivize the private sector or provide funding to an agency to do this through government. I mean, we need to know that.

Ms. ROSENWORCEL. I got an idea.

Chairman JOHNSON. OK, good.

Ms. ROSENWORCEL. By the way, I agree completely with everything that Chris just said at the end of the table.

I think the FCC set up something called "innovation zones" during the last several months in New York City and Salt Lake City, where it will be issuing experimental licenses for 5G. We should see how we can use those zones to start creating testbeds for more activity with Open Radio Access Networks and we should comb through our rules to see how we can incentivize that and make it happen, and certainly, with this Committee's help, I hope my colleagues would agree.

Chairman JOHNSON. Again, this is prodding coming from somebody who is not a real fan of government, OK? Really does believe in the private sector as being innovators, but again, we are in a competition with a command and control economy that is subsidizing and making it very difficult to compete. It is breaking down the marketplace. So we have to recognize that reality, but again, we need to understand what we need to do in a very complex environment.

So, again, there is going to be a lot more work. You are going to have a homework assignment after this hearing. That is one of the benefits of coming before this Committee.

Do you have some more questions?

Senator PETERS. Thank you, Mr. Chair.

Commissioner Rosenworcel, I just want to say I appreciate your passion on expanding broadband access everywhere. We have heard that today and in meetings prior to this as well.

I have certainly seen firsthand in my State of Michigan that access to broadband is as critical as clean water and electricity. We have to look at it that way to make sure everybody in this country, no matter who they are, no matter where they live, have access to that. Remember that a lot of rural areas do not have 4G now. So, to be talking about 5G, they are really very far behind. So I appreciate your comments on the mid-band as well as the mapping, and we have to continue to work in that area.

But my question to you is the FCC proposal would also bar communication companies from using support they receive from the universal service fund to purchase equipment or services from companies that pose a security threat.

So my question to you, Why is this proposal only focused on service providers using Universal Service Fund (USF) funds when the FCC has jurisdiction over the entire wireless industry?

Ms. ROSENWORCEL. This is a good question.

It is my understanding that based on the Executive Order, the Department of Commerce has an obligation to look at this issue more broadly across the economy, and so the FCC has focused on its distribution of $4.5 billion a year for rural America and making sure that those funds do not go toward insecure equipment.

But I believe that under the Executive Order, the broader choices in the economy fall to the Department of Commerce, and they were supposed to have rules, I think, by this month.

Senator PETERS. Anybody else care to comment?

Ms. RINALDO. Yes. On May 15th of this year, the President issued an Executive Order giving the Secretary of Commerce emergency authority to make determinations against transactions into our ecosystem through information communications technology and services. It gave him immediate authority. He could act today, if necessary, but we are currently working through the regulations, which lays out the process.

Senator PETERS. So there could be other funds that are being used besides just USF?

Ms. RINALDO. So there are no funds. This is just a procedural determination.

Senator PETERS. OK. So right now, just USF funds, though. If this is a national security threat, why would there not be other sources?

Ms. ROSENWORCEL. I am familiar with what the FCC is doing with the universal service funds——

Senator PETERS. Right.

Ms. ROSENWORCEL [continuing]. And I believe the broader obligations in the economy would fall to the Department of Commerce.

Senator PETERS. Are there proposals to prevent companies from using their own funding, non-Federal dollars, from purchasing Huawei and ZTE so they could be getting Federal funds, but as a result of that, now they can use their private funds?

Ms. ROSENWORCEL. Again, I believe that that would fall to the Department of Commerce.

Senator PETERS. Any thoughts on that area?

Ms. RINALDO. Yes. Again, we are currently moving through the drafting of the regulations, laying out the process.

Senator PETERS. OK. Just one final thought. We know—and I think there is some discussion as to whether we are behind or we are in a blip or wherever we are related to 5G, but we know we were the leader in 4G. And we were well ahead of everybody else. Now we are in a situation where we are debating whether we are behind or we are in a blip.

We want to make sure the United States is a leader in verging technologies on a regular basis, and we are at the verge of a massive explosion of emerging technologies that are coming on the market.

Going forward, is there something we should be thinking about, what we have learned from how we were leader in 4G, went to 5G, still trying to figure out how we get back ahead? Are there some lessons learned for emerging technologies generally that we should be thinking about right now as we approach this?

Mr. STRAYER. Senator, exactly. That is the bigger-picture issue that a lot of us are wrestling with now. You might know that we actually have an Executive Order on artificial intelligence——

Senator PETERS. Right.

Mr. STRAYER [continuing]. Basically the Artificial Intelligence Strategy, and that is composed of a couple elements. One is looking at how we advance R&D in the domestic markets as well as we

buildup a workforce that is going to be in that area, at the same time protecting our critical technologies from other countries, such as China, from acquiring those and using them for their military through their process of military civil fusion.

So we need strategies on each of these, and we are developing—we have strategies on 5G and now a strategy on AI, and I think that is how we have to address all of these. And we have to do it with our partners around the world that share the same values that we do because these are inherently discussions about how we are going to see data used by governments and by the private sector over a much longer term.

Senator PETERS. Well, I appreciate you bringing up AI. If you look at the investments that the Chinese are marking in 5G, those are probably dwarfed compared to what they are doing in AI. I understand that is one of the most transformative technologies coming forward. Mr. Krebs.

Mr. KREBS. It is not just about our investments and where we are putting our areas of focus, but it is also about ensuring a level playing field globally, thinking about how do we keep technologies that have been derived from theft or other nefarious means, how do we keep them out of the marketplace.

CrowdStrike, a couple weeks ago, released a report about a Chinese airliner that was cobbled together from 20-some-odd stolen technologies from a number of different countries. Is it fair? Is it equitable for that airframe to be in the global marketplace? These are the sorts of conversations that I think we need to tease out further.

Senator PETERS. Right. Yes.

Ms. RINALDO. I would also like to mention our work with the American Broadband Initiative. NTIA has been co-leading along with the Department of Agriculture (USDA) a plan on how we cut red tape on moving forward on the deployment. You mentioned rural areas. Currently, the Federal Government owns 30 percent of land in the United States. So how can we site? How can we build out fiber on Federal lands? As you know, fiber will underpin 5G. So these are some of the important issues that will help promote the deployment of 5G as well as help rural areas.

Senator PETERS. Commissioner.

Ms. ROSENWORCEL. Three things. First, we have an eight-page Executive Order on artificial intelligence. We need a national plan and a national strategy. Other countries have them with clear goals. We do not. We have to fix that.

Next, we need a smarter national spectrum strategy. A national strategy was due in April of this year. We still do not have one, and at the FCC, I think we are auctioning the wrong spectrum right now.

Then, third and finally, if Congress sees fit to ever pass an infrastructure bill, I think it would be important to incentivize municipalities to help with the streamlining of siting of terrestrial facilities required for next-generation wireless networks.

Senator PETERS. Great. Thank you. Thanks to all of you.

Chairman JOHNSON. Senator Hassan.

Senator HASSAN. Well, thank you, and thanks for allowing a second round of questions.

Thank you all for sticking with the hearing this morning. It has been a really helpful one.

I do want to note that this Committee passed a bill that Senator Warner and I had introduced on the Internet of Things security. It was a bipartisan vote, and it basically just said that if vendors want to sell IoT devices to the Federal Government, they have to meet certain cybersecurity standards. And it would be a very good way for us influencing the private-sector cybersecurity on those IoT devices.

We passed it out of this Committee. It has not been taken up for a vote on the Senate floor, and I think it would be a great thing for us to be able to do to help our commercial sector move forward in this way.

I wanted to follow up a little bit with you, Mr. Krebs, on the issue of ransomware. So thank you for your willingness to work with local, county, and State partners on this. Obviously, ransomware has been impacting government entities across the Country at all levels, including in my State of New Hampshire, where recently a county government was hit. Luckily, they had a backup plan. They recognized the threat. They shut down their systems, but they had to run a jail, a nursing home, and dispatch with pen and paper until they could get it back up. And everybody needs to, obviously, be prepared for that.

I understand that CISA has briefed State and local entities and has tried to share information with them about the nature of these threats, and that is certainly movement in the right direction. But I think we have to do more.

So beyond briefings and advisories, what is your agency doing right now to get resources and expertise to those entities that have either suffered these attacks or at risk of being targeted by ransomware attacks, and what help do you need from Congress to succeed in this?

Mr. KREBS. Yes, ma'am. Thank you.

Within CISA, we have a cadre of field professionals, whether cybersecurity or broader protective security advisors, that work day in and day out with State and local officials, sharing information, sharing best practices, reviewing response plans, reviewing architectures, trying to get them to a position where they can better defend their networks.

With more of those field professionals, I can have more reach and more engagement, and we are not talking about a dozen here or there. I am talking about a pretty significant uptick in folks out in the field. So that is something that we are working through right now.

I also think that we have to get to a point where we accept the fact that we are never going to be able to completely defend our way out of this. You are never going to patch every system. From a financial perspective, some folks just will not be able to keep up. They have, in fact, been left behind.

So what is industry doing to help fill the gap? How are companies shifting from a stockholder-centric approach to more of a stakeholder-centric approach and providing reasonable resources?

Then last thing, I think we need to be thinking much more about what we can do to disrupt these actors. So it is bigger than, again,

defending, but what is the role of other agencies within the Federal Government and the role they can play to stop these attacks before they actually happen and put the bad guys on the run?

Senator HASSAN. Thank you.

And then I wanted to come back to you, Commissioner, just to talk a little bit more about 5G.

You have heard it—and all of you have heard it from Members of this Committee and I think probably an awful lot of Members of Congress. We need to continue to turn to the needs of our rural communities when it comes to connectivity.

As Governor and now as Senator, I drive all around my State, and I can tell you where we do not have access to broadband to cell service. And I am as frustrated by our mapping deficiencies as anybody else.

We are all aware too, to Senator Peters' point, the benefits that 5G can bring. We have to get 5G right for Americans who live in rural communities, not just in our largest cities. To that end, I have reintroduced the bipartisan Advancing Innovation and Reinvigorating Widespread Access to Viable Electromagnetic Spectrum Act (AIRWAVES ACT) with Senator Gardner, which directs the FCC to auction valuable mid-band spectrum, to your point, Commissioner, and then to use some of those auction proceeds to fund rural broadband deployment.

Mid-band spectrum is crucial to developing a 5G architecture that works in rural areas, and making mid-band spectrum available will let companies innovate and develop new technologies that are suitable for rural deployment.

As the world looks for leadership on 5G standards and technologies, the FCC has an important role to play in ensuring that America is the preeminent voice on what 5G will look like and whom it will serve.

So, Commissioner, you have talked about this some, but I really would just like you to use this time to tell us anything you have not said about how the FCC plans to use its existing authority to free up mid-band spectrum for 5G use and how new technology can be used to drive down the costs of rural networks.

Ms. ROSENWORCEL. Alright. Thank you for the question.

Listen, there are a lot of places in this country that have no G's——

Senator HASSAN. Right.

Ms. ROSENWORCEL [continuing]. And getting to 5G is going to be a long way, and the reason they frequently do not have that infrastructure is that it is costly to deploy, and there are not a lot of people to spread the costs around.

Senator HASSAN. Right.

Ms. ROSENWORCEL. So the best way you can lower the cost is use the spectrum that propagates further.

Right now, the FCC has focused all of its early energies on high-band airwaves, the 24 gigahertz band, the 28 gigahertz band, the 37 gigahertz band, the 39 gigahertz band, the 47 gigahertz band, that propagate roughly 300 feet. There is no math that is ever going to make that effective in rural New Hampshire.

It could be interesting in discrete areas, but it will not be ubiquitous service, and it will not help the economy thrive, which is what you need.

So what we have to do now is reprioritize and start auctioning off mid-band spectrum. It is where the rest of the world is building 5G. We need to do it too. It is the spectrum that will get to everyone, everywhere, fastest, and most economically.

Senator HASSAN. Thank you very much, and thank you, Mr. Chair and Ranking Member Peters.

Chairman JOHNSON. Senator Portman.

Senator PORTMAN. Thanks. Thanks for allowing a second round.

So much here. One thing I am told that has not come up yet is looking at EINSTEIN and how it is working. Director Krebs, I am going to pose this question to you. EINSTEIN is an effort to ensure that our Federal agencies are protected from cyberattacks. We have EINSTEIN 1. We have EINSTEIN 2. We have EINSTEIN 3.A, I guess, or 3A. My understanding is that this current program, while effective in terms of the monitoring of the Federal networks, does not scan the cloud or traffic that comes in from mobile source. Is that correct?

Mr. KREBS. So EINSTEIN 3A, in particular, Domain Name System (DNS) sink-holing and email filtering is architected to traditional on-premise environment with an exchange server and things of that nature.

As we shift to the cloud and more agencies are shifting to the cloud, we are going to have to take a different approach.

We are having a number of conversations, both with the major cloud providers and email providers that work with the Federal Government on how we can get the transparency outcomes, the certain tags that we are looking for in email, in particular. The progress we are making is noteworthy.

But we are accelerating quickly into the cloud, and we are going to have to take a different approach.

There is a recent policy, TIC 3.0 policy, and we are going to be sending out an additional security architecture baseline behind that in the next month or so, I think.

But, again, we are working through what some of the alternative architectures look like for cloud. I am very much interested and vested in this space, less about putting a physical device on a network and more about what do a few lines of code look like in the Azure marketplace, in the Amazon Web Services (AWS) marketplace, to get, again, the information that we need to ensure that government clouds are protected.

And I would add that these are the sorts of capabilities, as we build them out and refine them for the Federal Government, we should also be thinking about how they scale to State and local governments, with the appropriate privacy protections in place.

We have similar capabilities under the Albert program for NetFlow and intrusion detection systems. How are these things also able to assist State and local capabilities as they also move to the cloud?

Senator PORTMAN. You just raised a whole other issue, which is State and local government, which is a huge problem as well. But we are glad you are there. You have experience working in the pri-

vate sector on companies that are very active in the cloud, and we want to be helpful. So let us know.

As the Chairman said earlier, if there are any impediments to that—because you are right. This is where so much of what we should be concerned about in terms of cyberattacks is moving, and yet EINSTEIN, for all of its good work 10 years ago, is not keeping up with the technological changes. So let us know if we can help you to accelerate that.

On the State and local side, since you mentioned that, there is legislation that has been reported out of this Committee. We are patting ourselves on the back a lot on this Committee today because we have actually reported out some good stuff.

Senator Peters, you were the coauthor of this legislation, and it basically says what you just said, which is we need to help State and local more. It is called the State and Local Cybersecurity Act. It would authorize you guys to work with some of these groups, including with the Multi-State Information Sharing and Analysis Center, and I know you are already doing this. This gives you the clear authorization to do it, to be able to help our State and local partners.

I guess one question I would have for you is, what opportunities exist to partner with some of these nonprofits to protect against the Chinese threats in the 5G space?

Mr. KREBS. So that is a conversation we are having. Again, I mentioned the Denver event, the Rural Engagement Initiative, where we met with a number of rural providers and some of their trade associations on how we pull together kind of a best practice guide and playbook for how these rural organizations might be able to shift into a non-Huawei, non-ZTE environment.

What we have to do is distill down some of the investments that the larger carriers have made, the successes, the best practices they have developed, and then we have to push those down as far as possible, because you are just simply not going to find the ability to invest the way some of the larger carriers—so how do we, again, harness that investment, how do I distill down my own insights as a cybersecurity agency and then put into easy-to-apply playbooks and frameworks for these agencies or these carriers to do the things they need to do.

Senator PORTMAN. Well, again, we want to be helpful in that, and we think it is timely.

One final question to Ms. Rinaldo because you have not gotten any questions in a while. [Laughter.]

We were talking earlier about your work on the expansion of broadband into rural areas, and you mentioned working with the U.S. Department of Agriculture.

In the Farm Bill last time, we also had legislation that came out of this Committee, at some point, maybe focused more on the rural communities, and the focus is to give them the ability through a new commission and so on to do more in terms of broadband.

We also have legislation to help the co-ops do more, called the Rural Act, because right now under our new tax law, there is some confusion as to whether co-ops might lose their tax-exempt status if they get involved in broadband.

Can you tell us a little more about what you are doing, one, with Department of Agriculture, and has the Farm Bill legislation helped, to your knowledge? And, second, with regard to co-ops, are you working with rural co-ops at all in expansion of broadband?

Ms. RINALDO. Sure. So our current work with the American Broadband Initiative involves helping coalesce more than 20 different departments and agencies on what we can do as a government to help break down barriers, and as I mentioned, 30 percent of lands are federally held. So, as to their siting, can we build fiber? We are also looking at how money is spent.

We recently created a tool on our website where you can go for a one-stop shop to see where Federal grants—I have not worked particularly with co-ops, but I am happy to take that back. And I will get you an answer, and I will be happy to sit down with your staff and go over more of the work that we are doing in that area.

Senator PORTMAN. Well, if you could, that would be great.

Ms. RINALDO. Absolutely.

Senator PORTMAN. They are a natural partner in this, and they have the interest and ability, just as they have had with electricity. Now it is broadband. So we would appreciate that.

Thank you very much, Mr. Chairman.

Ms. RINALDO. Thank you.

Chairman JOHNSON. Senator Portman, I was at an event earlier this morning on 5G, and there was a former mayor that was involved in one of these 5G test site cities. He was talking about the resistance from the population of putting up the antennas.

Also mentioned, apparently, there are Russian bots that are out there putting out false information in terms of the health dangers of 5G.

I just want to ask you. First of all, is that true? Second, do we have in any of your agencies, the research to refute that, and are you publicizing that?

Mr. KREBS. So I am generally aware of open-source reporting that Russian disinformation campaigns are promulgating the concept that 5G is a dangerous technology.

My agency is focused on raising public awareness of disinformation campaigns and misinformation campaigns, how they work, and the things that individually you can do as a consumer of media, social media, traditional media, or otherwise of spotting these sorts of campaigns and not contributing and doing their work for them.

This is going to be the battlefield really of the future. It is easy to invest. It is low level of investment, broad coverage, and it is really hard to stop.

So while the intelligence community and the Department of Defense are on the operational disruption side, we have to do a lot more, I think, in terms of engaging the public on helping them understand how these things are happening and kind of how the Russians and others, increasingly Iranians, Chinese, are trying to hack our brain to get——

Chairman JOHNSON. It is really kind of a twofold counter. First of all, I just point out the fact that Russia is engaged in this type of disinformation, but then we need to provide the accurate information. We need to have the research to put the public's mind at

ease on this. Do we have that research? Are we pushing that out, either through the Department of Commerce or through the FCC?

Ms. RINALDO. I am not familiar with a particular white paper on this.

I know through our broadband work that we are in the communities doing seminars, webinars, with local communities to counteract any information that might be out there. So I am happy to dig a little deeper and see if there is a report available.

Chairman JOHNSON. Commissioner, do you know of any effort?

Ms. ROSENWORCEL. Well, I too have seen news reports like the ones you suggest, and the FCC does have an open proceeding on some of these issues.

But I would also say this. In the bigger picture, if we want to get the facilities deployed on the ground everywhere in this country, we are all going to have to figure out how to work with States and localities to do so.

We have a 10th Amendment in this country. We treasure our local control, and we are going to have to figure out how we are all rowing in the same direction. And that is going to take some work.

Chairman JOHNSON. Well, that particular State passed a preemption law so that all the communities can do it.

Ms. ROSENWORCEL. OK.

Chairman JOHNSON. Again, we also have to provide accurate information. We need to understand that this disinformation is out there, and we need to have a program for that.

Commissioner, you talked about the FCC's seal of approval or whatever. Again, with the Internet of Things, you are going to have an explosion of devices. Do you have the capacity and capability of providing that type of approval for all these devices? Is there something in place, or can you envision something in place to do that?

Ms. ROSENWORCEL. That is a good question. It is so radical, the increase we are going to see in connected devices. By the end of the decade, we could have 20 billion things that are connected worldwide.

For the FCC, this is a challenge because we are going to have so much more that is connected, but one thing I would point out is that we do have a process in place where the agency itself is not the only one certifying that these devices are safe and effective. We often do that through third-party certification bodies.

So what we are going to have to do, though, is identify new ways to streamline this work, but I think we should also look at that process and see how we can build security into it from the get-go, so our authorization is not strictly about interference but also is about security.

Chairman JOHNSON. So my suggestion would be the government help write standards through NIST or whatever and then using underwriter laboratories or those types of private sector——

Ms. ROSENWORCEL. Yes. And that is historically how we have done a lot of these authorizations. If there is a totally new use of spectrum, the FCC will take a look at it, if there are new devices with new capabilities.

But once devices become routine, it typically shifts to a certification model done through third parties, and I think that that process could serve us, though it will be bigger in this environment.

Chairman JOHNSON. Director Krebs, you talked earlier about the airplane cobbled together with all of the stolen technology. One of the questions I have is just patents. Are we going to challenge or is there an effort to challenge some of these? You say that China holds, what, 34-some percentage, a pretty high percentage of the patents around 5G. Are those valid patents? To what extent are those patents based on previously stolen intellectual technology, and is that one of the ways we can potentially combat them in terms of just not recognizing some of those patents?

Mr. KREBS. Extending out of my lane here for CISA, but I think this is a reasonable path to do patents that are issued in China, do they matter on a global scale.

Chairman JOHNSON. Anybody else want to weigh in? Mr. Strayer.

Mr. STRAYER. Yes, Senator. All patents are going to have the same impact over the long term of the ecosystem, and I think it is a little overstated about the success of China in this area. We have a report out today that says that Intel, Qualcomm are leading with the patents that will be the most valuable for the 5G ecosystem.

China has definitely played in a lot more teams that are fielding. So there will be a consortium of companies that come together, and Huawei and others will put their people on that team just so they can take credit for that and tick that up in their count.

So I just would recommend a little caution in some of the public debate about how you arbitrate where success lies in this.

Our companies seem to be doing just fine overall, but as I said before, we need to be vigilant about how we participate and how we exercise control over the multilateral institutions that set up other frameworks that set the rules for participation and the later specifications that are developed under those.

Chairman JOHNSON. I am all about recognizing reality as it actually exists.

One of the things, we were talking about the buildout, the 150,000 in antennas already deployed in China. In the end, that is really not that big a deal. These are pretty small little antennas. They do not cost that much.

We are trying to build out these individual cities, really get the technology down right, know how to do it. The Chinese just may have wasted a lot of money putting up 150,000 antennas that are not going to really be all that useful. Is that a relatively accurate statement?

That in itself does not scare me. It is a scary number, but in actuality——

Ms. ROSENWORCEL. Sure. I think it is a useful data point. It tells us that they are ahead.

Chairman JOHNSON. Oh, yes. They are aggressive.

Ms. ROSENWORCEL. It tells us that South Korea is ahead too when it comes to deployment, and one thing about technology is that deploying early and at scale gives you leadership opportunities. So I think we need to be mindful of it.

Mr. STRAYER. Senator, if I could just weigh in on the point about us, we are leading on 5G. Using the standard of how many towers deploy in the field is not accurate.

Just 2 months ago, China put in licenses for its operators to do 5G. So there is no way they could already be deploying 5G. They built towers for it, but they just gave out the licenses to the companies.

We have it in more than three dozen cities in the United States. We are leading in 5G. South Korea is right there with us.

I am not saying we should not pay attention to competitors in the space, but a lot of this falls from the Chinese Communist Party and Huawei working so closely together to push out millions of dollars of propaganda through all kinds of means around the world, and I just want to let out——

Chairman JOHNSON. China also leads in terms of producing these massive ghost cities.

Mr. STRAYER. Yes. And they——

Chairman JOHNSON. Again, their system misallocates capital, but, again, they can also be very strategic. And they can subsidize and really hurt a free-market competitive system as well. Ms. Rinaldo.

Ms. RINALDO. I would just echo that it is population density. When it comes to patents, it is quality over quantity. It is my understanding that we are going to have more than 100 cities built out by the end of the year. So we are firing on all the points that we need to be.

Chairman JOHNSON. OK. Magically, my time never even started, so I still got 7 minutes.

Let me close this out, though, by kind of getting back to where I started, the problem-solving process, gathering information, defining the problem, the opportunity of the problem, but then establishing achievable goals.

So, again, what I wanted to come out of this hearing, the goals, what can this Committee do? What can Congress do in terms of priorities that we need to set, the goals we have to establish as you are continuing down your paths? What can we do to help you? Can we kind of get some answers on that?

Let us start with spectrum. I will go back to the homework assignment. If there is any roadblocks that we can help knock down, either legislatively or just with oversight letters or shine a big old bright light on it, "OK, guys. Let us get this resolved, and let us move forward." That is kind of what I want out of the close-out statement.

So why do not I start with Director Krebs. What are those top three things, let us say? If you really got five, go ahead, but what are the top three things you would like this Committee, you would like Congress to do in terms of achieving your priorities and your goals?

Mr. KREBS. At the top of the list right now is make it easier for companies to share information on risky vendors that they come across and make it similarly easy for me to share that information. I do not want to ever have to go through another Kaspersky Labs antivirus product situation. We need to be able to rapidly get information out.

Second is make it easier for me to be able to convene groups to develop frameworks, to share more broadly.

Chairman JOHNSON. Why do you have a difficult time now? Just because of antitrust?

Mr. KREBS. There are some antitrust issues involved here. I am restricted to some of the Sector Coordinating Councils (SCC) at this point in terms of those trusted convening mechanisms. So I think we can take a harder look at the way we pull groups together.

And third and finally, we are working on an administrative subpoena proposal right now with your Committee. That is a big priority for me. Once we identify vulnerable systems out there, whether it is industrial control systems or telecommunication systems, we need to be able to get to the people that are managing those systems so that we can close down those vulnerabilities before a bad guy gets to them.

Chairman JOHNSON. I am quite sure that piece of legislation is on our markup next week.

Mr. KREBS. Good to hear.

Chairman JOHNSON. Hopeful to get that passed with strong bipartisan support——

Mr. KREBS. Excellent.

Chairman JOHNSON [continuing]. And then figure out some way to wind it through the congressional process to get that signed into law.

Mr. KREBS. Thanks for your support.

Chairman JOHNSON. Ms. Rinaldo.

Ms. RINALDO. I would say, first, as you talk to business leaders around the country, encourage them to participate in standards-setting bodies.

Second, as you talk to your constituents, tell them about—alleviate any concerns they might have—about 5G. Talk to them about the benefits of it.

Third, keep doing things like this. Keep having hearings. The underlying element of my three points is education. I believe education is the unsung hero in this debate.

Chairman JOHNSON. OK. Mr. Strayer.

Mr. STRAYER. Thank you for that question.

One thing that we have been working on at the State Department is creating the architecture internally so that we can be full competitors with China and Russia and others in emerging technologies. So we propose that there be a cybersecurity and emerging technologies bureau. That proposal has been sitting up here in Congress for the last 5 months under review in the Senate Foreign Relations Committee. If you could help facilitate——

Chairman JOHNSON. Which I do not chair.

Mr. STRAYER. Yes. But you might know some of the other Senators there.

Chairman JOHNSON. OK.

Mr. STRAYER. We would want to engage in a real dialogue about how we can set up an emerging technologies bureau that will make us able to fully work with our partners, our key like-minded partners on emerging technology issues and developing the strategies of the future because we are not going to have all the solutions in the United States. So we really need to be equipped at the State

Department to be able to engage in future discussions with our key partners, and part of that is resources in that, and part of that is the imprimatur that we are a major part of the Department's effort in the future of digital technologies.

The other thing I just want to mention was we really appreciate the financing we get through foreign assistance money that can help us work with other governments on their deployment of trusted technologies in both 5G and future connected technologies.

And, last, I would just say the way that I think you all have a united view about the threat and the risk from these types of vendors and if you are enabled or in a position to share that in CODELs and other places with interlocutors and other governments and with legislators around the world, that it would be very helpful to us as we do our own messaging efforts in that regard.

Chairman JOHNSON. Just a quick comment. A year ago, as we are visiting all of these delegations, nobody really understood Huawei. At least now they have the knowledge of it, and it sounds like they are starting to take action on it as well. Maybe not fully as much as we want, but we have come quite a long ways from complete ignorance of the issue and the problem to not only not acknowledgment of it and taking steps to alleviate it.

Mr. STRAYER. Completely agree. Thank you.

Chairman JOHNSON. Commissioner.

Ms. ROSENWORCEL. Thank you.

First, we need a national spectrum strategy, not just for this year or next, for the long haul, and it is going to have to have incentives for Federal actors to relinquish airwaves for commercial purposes over time. The absence of those incentives slows us down.

Second, we need broadband mapping, and Senator Peters knows this. We cannot manage a problem if we do not measure it, and we are not measuring broadband in rural America right now. I think it is going to have chilling effects for both national and economic security.

Third, anything we can do to help with network virtualization and the Open RAN is something we should invest in. It is a way to help us manage the supply chain challenges going forward.

Then, fourth, and this is just adjacent, but I think it is important—we do not have a national artificial intelligence strategy. Other nations do. We need one.

Chairman JOHNSON. And what about quantum computing?

Again, this hearing is so within this Committee's mission statement. Our top priority is border security but then cybersecurity, protecting critical infrastructure, countering violent extremism, which is more and more often done online. This is something we will continue to be fully engaged with. We want to be engaged.

So, again, I am just asking all of you to work very cooperatively with not only Members, but our staffs, and we will keep pushing the ball forward. Any time you need any help from this Committee or Congress, please do not hesitate to ask, and we will do whatever we can do.

I got to get the magic words here. Thank you again for your time, your testimony. I thought this was an excellent hearing, and again, it is just a start.

The hearing record will remain open for 15 days until November 15th at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 11:32 a.m., the Committee was adjourned.]

APPENDIX

Chairman Ron Johnson Opening Statement
"Supply Chain Security, Global Competitiveness, and 5G"
October 31, 2019

We are at a technological crossroads. While the development of 4G wireless technology made innovations like Uber and Netflix possible, the transition to 5G promises connectivity that is 100 times faster and five times more reliable. It will also enable us to connect exponentially more devices at the same time, a capability that will empower the Internet of Things, which will inter-connect all modern devices, as well as innovations like artificial intelligence and smart cities.

But this progress is not inevitable. According to FBI Director Christopher Wray, the vulnerabilities associated with the development and deployment of 5G technology, especially the threat posed by China, is one of the "generational threats that will shape our nation's future."

That threat relates both to national and economic security. When it comes to cyber attacks and cyber espionage, China is a known bad actor. China was responsible for the 2015 OPM data breach and is suspected to be behind other high-profile security breaches, like the Anthem and Marriott breaches. Whether highly-sensitive and classified national security information or the private information of American consumers, China will do whatever it can to steal information from competitors. Recognizing China's intent and its domestic laws requiring its companies to do whatever is asked of them, there is serious cause for concern with having a Chinese-backed telecommunications company responsible for major components of 5G networks.

With regard to our economic security, winning the race to 5G is worth billions of dollars for the U.S. economy. It is imperative that the U.S. maintain its global leadership with 5G and not let adversaries like China and other competitors seize the first-mover's advantage, which includes setting the standards for a host of related technologies, and the related economic benefits.

How are we, as a nation, planning to address the threat posed by China and ensure we win the race to 5G?

At the outset, it is imperative to recognize that the federal government cannot do this alone. Although recent legislation and an executive order include efforts to secure the federal government against threats posed by Chinese information communications technology, or ICT, companies, the vast majority of this risk rests with the private sector and state or local governments. The federal government must work in coordination with private sector experts to ensure that we have the processes, authorities, and resources necessary to address the challenges inherent in this effort.

These challenges are not restricted to the homeland. Even as the U.S. works to secure its own infrastructure, our increasingly interconnected world means that the U.S. is also at risk from the vulnerabilities in the wireless networks of other countries. Any country whose ICT supply chains run through China, a nation that uses cyber espionage as a way of doing business, is at grave risk. Thus, because of the nature of the problem, any true solution must be comprehensive, which requires the U.S. to act in concert with its international allies and partners.

The U.S. must also confront the reality that some allies and partners will not or cannot avoid entirely the use of Chinese ICT from essential parts of their 5G networks. What should we do in those instances?

This is an extraordinarily complicated task, but to make matters more challenging, I am not convinced that we have a consensus between the various federal government agencies on what the problem is that we are trying to tackle.

I am a businessman—a manufacturer—and one of the most important things I learned in that job is the value of strategic thinking and planning. But access to the most sound and creative thinking means little without the ability to transform it into action. To do that, we must be able to answer foundational questions: Who's in charge of guiding these complex conversations and making the tough decisions? Who will define what "success" on 5G looks like from a national security perspective?

Generational problems cannot be solved without a shared understanding of the problem and an agreed-upon approach for addressing it. I look forward to discussing how we can work toward these goals with the witnesses here this morning.

U.S. Senate Committee on Homeland Security and Governmental Affairs
"Supply Chain Security, Global Competitiveness, and 5G"

OPENING STATEMENT OF RANKING MEMBER GARY C. PETERS
OCTOBER 31, 2019
AS PREPARED FOR DELIVERY

Our modern economy is truly global. Internet access is no longer a luxury. It is a necessity, and a vital tool that connects people with educational opportunities, creates jobs and drives economic development.

The introduction of 4G technology brought us live-streaming, ridesharing, on-demand delivery, and other innovations. And now, the 5G era is at hand.

This faster, stronger wireless connection will once again transform our digital world, enabling new technologies like precision agriculture, self-driving cars, and augmented reality.

5G networks and the new technologies they spur will create countless new jobs in Michigan and generate billions of dollars in economic growth across our country.

5G has the potential to unleash new productivity and help cement the United States as a global leader in innovation. But developing the infrastructure needed to support 5G networks across the country does not come without risks.

Today, China, arguably our nation's greatest global competitor, is poised to lead the world in advancing this important technology.

China's edge in the development of 5G equipment and standards poses a threat to both American economic dominance and to our national security. The U.S. is increasingly reliant on high-speed telecommunications services to support not only our broader economy, but also our entire defense industry.

In the race to expand 5G access, we face serious supply chain security risks by purchasing and deploying Chinese-made equipment from companies like Huawei and ZTE, companies our Intelligence Community has said may be beholden to the Chinese government.

The devices these companies provide potentially offer cost-effective solutions to help close the digital divide. But they also pose a serious national security risk and could open a backdoor into critical American security networks.

Given these serious national security risks, we must navigate a delicate balance of ensuring that emerging 5G networks are both secure and widely available in rural and urban areas.

China's advantage in 5G may be a reality for now. But it is also something that we have the power to change.

The United States government, including this Committee, has an opportunity to play a key role in America's resurgence as a leader in the development of 5G networks. A challenge of this magnitude requires a strong, unified and collaborative approach – capitalizing on the full power of American ingenuity.

But to date, our efforts have been piecemeal and disorganized. We do not have the dedicated leadership or the coordinated national strategy needed to accomplish this critical mission. I am encouraged by the bipartisan agreement this Committee has made to support this goal.

Universal 5G connectivity would encourage renewed prosperity in both urban and rural communities, unlock tremendous economic growth, and reestablish America as a leader in global innovation.

I hope that this hearing will serve as a driving force to help usher in a new era and build momentum towards recapturing our place as the world's leader in communications technology.

Thank you.

Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

Supply Chain Security, Global Competitiveness, and 5G

BEFORE THE
UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT REFORM

October 31, 2019

Washington, DC

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you for today's opportunity to testify regarding the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) ongoing efforts to secure our telecommunications infrastructure. Thanks to Congress's leadership and passage of the *Cybersecurity and Infrastructure Security Agency Act of 2018* (P.L. 115-278) nearly one year ago today. CISA is now even better poised to achieve our important critical infrastructure security and resilience mission.

Understanding the Threat

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states, increase the frequency and sophistication of their attacks. In a 2018 report, *Foreign Economic Espionage in Cyberspace,* the U.S.'s National Counterintelligence and Security Center stated, "We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace." Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

During his annual Worldwide Threat Assessment testimony before Congress this January, the Director of National Intelligence stated, "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies." The Director further stated, "We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies." This assessment is consistent with the fact that Chinese laws on national security and cybersecurity provide the Chinese government with a legal basis to compel technology companies operating in China to cooperate with Chinese security services.

Increasingly, many or most discussion around cybersecurity threats include some risk calculation around supply chain, third party, or vendor assurance risk. In fact, a 2018 Symantec report detailed that the number of observed supply chain attacks was 78 percent higher in 2018 than it was in 2017, as malicious actors sought to exploit vulnerabilities in third-party software, hardware, and services.

Supply Chain Risk can broadly be understood as efforts by our adversaries to exploit ICT technologies and their related supply chains for purposes of espionage, sabotage, and foreign interference activity. Vulnerabilities in supply chains – either developed intentionally for malicious intent or unintentionally through poor security practices – can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system and network failure. Increasingly, our adversaries are looking at these vulnerabilities as a principal attack vector, and we are increasingly concerned with aggressive actions, by potential foreign adversaries to include Russia, China, North Korea, and Iran.

Roles and Responsibilities

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the Department published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts.

CISA works across government and critical infrastructure industry partnerships to lead the national effort to safeguard and secure cyberspace. We share timely and actionable classified and unclassified information as well as provide training and technical assistance. Our work enhances cyber threat information sharing between and among governments and businesses across the globe to stop cyber incidents before they occur and quickly recover when they do. By bringing together the intelligence community, law enforcement, the Department of Defense, Sector-Specific Agencies, all levels of government, the private sector, international partners, and the public, we are enabling collective defense against cybersecurity risks, improving our incident response capabilities, enhancing information sharing of best practices and cyber threats, strengthening our resilience, and facilitating safety.

In addition to our cross-sector leadership role, CISA is the Sector-Specific Agency for numerous sectors, notably the Information Technology and Communications Sectors. In this role, we work with a range of stakeholders to address both short-term and longer-term challenges regarding risks to telecommunications networks, including supply chain risk management and 5G security. These stakeholders include the Department of Justice, Department of Commerce, Department of Defense, Federal Communications Commission, General Services Administration, the intelligence community, and the private sector.

To manage and address the risks posed by 5G, the U.S. government is taking an interagency approach to this issue, led by the White House. National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) - 4 process. These meetings are an opportunity to discuss and come to decisions on key 5G issues, such as participation in standards bodies, as well as to provide updates on interagency 5G activities.

Reducing ICT supply chain risk is a national security imperative and one that is a key pillar of CISA's Strategic Intent. While many components of CISA play some role in supporting supply chain initiatives, the National Risk Management Center (NRMC) leads the agency-wide supply chain coordination effort – providing program management and analytical support to current lines of effort. These include:

- The ICT Supply Chain Risk Management Task Force

- ICT analysis in support of Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain
- 5G mobile communications security and resilience efforts

CISA's supply chain risk management efforts are closely integrated with the agency's broader critical infrastructure protection mission. Supply chain risk cuts across many of the 55 National Critical Functions released by CISA in April, and the National Critical Functions framework continues to be an effective platform for holistically understanding and prioritizing risk to our nation's critical infrastructure.

ICT Supply Chain Risk Management Task Force

In 2018, CISA established the Information and Communication Technology Supply Chain Risk Management Task Force as a public-private partnership jointly chaired by CISA and the chairs of the IT and Communications Sector Coordinating Councils. The Task Force is working to identify and manage risks to the global ICT supply chain and is comprised of 40 industry partners from the IT and Communications Sectors and 20 interagency partners from the United States Government.

The first year of the Task Force focused on four priority areas of policy concern for supply chain risk management, including: Information Sharing, Threat Evaluation, Qualified Bidder Lists and Qualified Manufacture Lists, and Policy Recommendations to Incentive Purchase of ICT from Original Equipment Manufacturers and Authorized Resellers.

In September of this year, the Task Force released an Interim Report providing a status update on activities and objectives of the Task Force. The report outlines the overall structure of the Task Force as well as the four Working Groups, areas of discussion, and relevant key findings. The Interim Report serves as an important building block for the second year of the Task Force, including strategic priorities and recommendations.

Among these priorities is enhancing the information sharing about supply chain risks with a particular focus on potential bad actors. The Task Force identified current gaps in the ability of government to collect relevant information on bad actors, the ability to use that information as part of an overall evaluation of trusted vendors, and the ability for that information to be shared with the private sector. Crucially, the Task Force also identified limitations on private-to-private information sharing on supply chain risks because of lingering legal concerns. Going forward, the Task Force is establishing a Working Group of lawyers from industry and government to address these hurdles and make recommendations for legal and regulatory changes; in addition, the Task Force is likely to identify the necessary components of an enhanced information sharing environment that can take advantage of factors that contribute to understanding as to whether vendors can be trusted.

Another effort of the Task Force will be related to taking the output of a list of the Threat Evaluation Working Group – which identified nine types of supply chain threats and related scenarios – and making recommendations as to how the identified threats and threat scenarios can inform risk management programs for government agencies, and large and small businesses

alike. These threats – whether from counterfeit parts, insider threats, poor cybersecurity practices, or market forces – need to be accounted for in effective supply chain risk management programs.

In addition, to its Working Groups, the Task Force has emerged as a key private sector touch point for the recently launched Federal Acquisition Security Council (FASC). All agencies participating in the FASC also have representatives on the Task Force – a deliberately designed synergy. And, we recently completed an agency-wide data call for the FASC and the Task Force that identified supply chain risk management programs from across government for the purpose of increasing integration and synchronization of efforts across the Executive Branch.

ICT Criticality Analysis

On May 15, 2019, the President signed Executive Order (EO) 13873: Securing the Information and Communications Technology and Services Supply Chain. This EO declares a national emergency with respect to the threat posed by foreign adversaries to the nation's information and communications technology supply chain. Specifically, the EO addresses concerns that "foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States."

DHS, specifically CISA, plays a key role in EO 13873. Section 5(b) requires the Secretary of Homeland Security to "assess and identify entities, hardware, software, and services that present vulnerabilities in the United States that pose the greatest potential consequences to the national security of the United States." The Secretary of DHS, in coordination with sector-specific agencies and coordinating councils as appropriate, was required to submit an assessment within 80 days of issuance of the EO and annually thereafter. The assessment was required to include an "evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636."

The Secretary of DHS delegated this responsibility to CISA. To carry out this responsibility, CISA has engaged with its federal and private sector partners to provide assessments of ICT hardware, software, and services to determine which pose the greatest threats and vulnerabilities to US critical infrastructure.

CISA will soon release the methodology it used in its assessment in support of the EO. The methodology includes a deconstruction of the ICT supply chain into 61 elements – the hardware, software, and services "building blocks" – that collectively make up the ICT ecosystem. CISA hopes that this elemental deconstruction will have lasting value for supply chain risk management activity beyond this EO.

Among the elements that CISA designated as critical for focusing supply chain risk reduction efforts were Home Subscriber Services, Mobile Switching Centers, and Sensitive Systems Software (to include software defined networking). Untrustworthy equipment in those supply chains could create an unacceptable amount of risk to the national security of the United States. There would likely be significant regional or national impacts, including affecting operations and the confidentiality, integrity, or availability of data or the system, and the ability to effectively mitigate these risks is uncertain or unsatisfactory.

5G

With that finding in mind, DHS – and our interagency partners – recognize 5G deployment as a significant area for national and economic security intention. The Fifth Generation Communications Network (5G) is the next generation of wireless technology that represents a complete transformation of telecommunication networks. Combining new and legacy technology and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology.

From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow.

5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services. The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT), ultra-low latency required for critical near-real time data transmission, and faster speeds to support emerging technologies. As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States.

DHS, working with its interagency and industry partners, has an opportunity to help shape the rollout of this emerging critical infrastructure, increasing its security and resilience at the design phase and reducing national security risk from an untrustworthy 5G network. Our intent in doing so is to promote the development and deployment of a secure and resilient 5G infrastructure that enables enhanced national security, technological innovation, and economic opportunity for the United States and its allied partners.

Our work in this area will be focused on six lines of effort, to include:

- Support the design and deployment of 5G networks with security and resilience in mind, to include investing in Research & Development
- Promote 5G use cases that are secure and trustworthy
- Identify and communicate risks – including supply chain risks – to 5G infrastructure
- Promote development and deployment of trusted 5G components
- Advance the United States' global effort to influence direction of allied nations in 5G deployments

- Provide leadership role within USG to coordinate operational 5G security and resilience efforts

The analogy of the space race is not entirely incorrect for 5G deployment, but I view it more as a competition between differing views of the world – one in which technology is deployed that protects the values of privacy, enables greater confidence amongst citizenry in essential services, and creates greater connectivity and economic opportunity while not undermining the ability of countries and communities to protect themselves; and, one that views technology as an enabler of illegitimate behavior.

The United States' goal needs to be to do whatever we can to lead the world to the former vision. Industry will be a partner in all of this effort – so, too, will like-minded countries. One particular focus needs to be on ensuring that state-influenced entities do not dominate a market through unfair business practices and to potentially do the work of adversary action. As such, a particular concern that the Department of Homeland Security is focusing on regards the growing presence of Chinese telecom equipment in the Radio Access Network (RAN) portion of the network where there are a limited number of RAN equipment suppliers. There are five main purveyors of 5G RAN technology globally, the largest of which is Chinese-based. If Chinese manufacturers continue to gain market share, there will be growing concern about the long-term viability of the existing supply chain for 5G and successor technologies. As such, it is important for the U.S. and its allies to continue to promote market dynamism and support existing trusted-vendors in the space while investing in innovation and research and development that will help the trusted community win the quality battle in the RAN, innovate to a future 5G, and compete on a level playing field in the market. This is particularly necessary to help support deployment across the United States, including in rural communities.

DHS Advisory Conncils

CISA is working through the Critical Infrastructure Partnership Advisory Council (CIPAC) structure to engage with private sector stakeholders, especially the Communications and Information Technology Sector Coordinating Councils and the Enduring Security Framework Operations Working Group to collaborate on the risk posed by 5G technologies.

CISA operates the Communications Sector Information Sharing and Analysis Center (ISAC), a partnership of 11 federal agencies and over 60 private sector communications and information technology companies. Some of these companies maintain a permanent presence in CISA's operations center. Through the Communications ISAC, government and industry exchange vulnerability, threat, intrusion, and anomaly information. CISA also uses this mechanism to maintain situational awareness regarding the evolution of 5G standards and carrier 5G plans.

The President's National Security Telecommunications Advisory Committee (NSTAC), created in 1982, provides industry-based analyses and recommendations to the President and the Executive Branch regarding policy and enhancements to national security and emergency preparedness (NS/EP) telecommunications. It is composed of up to 30 presidentially appointed

senior executives who represent various elements of the telecommunications industry. NSTAC is supported by the Secretary of Homeland Security, who is the Executive Agent.

NSTAC has reviewed 5G security issues, including when it finalized its *NSTAC Report to the President on Emerging Technologies Strategic Vision* on July 14, 2017. The report included recommendations on how the government can adapt to "unprecedented growth and transformation in the technology ecosystem over the next decade," including 5G technology, which the NSTAC identified as a near-term transformative technology.

The NSTAC is currently examining technology capabilities that are critical to NS/EP functions in the evolving ICT ecosystem. On April 2, 2019, the NSTAC submitted a letter to the President outlining the first phase of its study to identify the technologies within the ICT ecosystem that are most critical to the Government's NS/EP functions, which include 5G, quantum computing, and artificial intelligence.

During the second phase of this study, the NSTAC plans to examine how certain dependencies, market limitations, and supply chain risks began, using the deployment of 5G technologies as a case study. The NSTAC will formulate recommendations for the recommended national innovation NS/EP ICT strategy. This strategy will ensure that the United States is more resilient, has access to trusted technology to support its NS/EP mission, and leads in the development and use of ICT technology.

Research and Development

The next age of digital transformation depends on the success of the United States' national and global 5G build out. Significant research remains to be done in this area as well as hardening of the 5G network protocols, which are currently in early development. On April 22, 2019, DHS's Science and Technology Directorate and CISA announced an effort related to the development of new standards to improve the security and resilience of critical mobile communications networks. This solicitation established a research and development project for innovative approaches and technologies to protect legacy, current, and 5G mobile network communications services and equipment against all threats and vulnerabilities.

The 3rd Generation Partnership Project (3GPP) and the United Nations' International Telecommunications Union (ITU) lead the global 5G standards development initiatives. CISA currently works with industry, including nationwide US wireless carriers, in preparing technical standards for the standards development organizations to ensure Public Safety and NS/EP personnel will have priority communications services on 5G networks.

Conclusion

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities

around cyber-physical risk and cross-sector critical infrastructure interdependencies.

A holistic understanding of critical infrastructure risk must take into account the supply chain risk stemming from an interconnected society that relies heavily on ICT technology as the supporting backbone of many National Critical Functions. As CISA continues to mature its engagement on supply chain risk management and 5G security and resilience lines of effort, the agency is also working on developing a lasting technological architecture and framework to allow for better structured supply chain risk analysis. We believe investing in this capability will be critical to fully achieving CISA's critical infrastructure mission in the years to come.

I recognize and appreciate this Committee's strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient Homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

TESTIMONY OF DIANE RINALDO

ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION (ACTING)

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
(NTIA)

U.S. DEPARTMENT OF COMMERCE

HEARING ON SUPPLY CHAIN SECURITY, GLOBAL COMPETITIVENESS, AND 5G

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

October 31, 2019

Chairman Johnson, Ranking Member Peters, and Members of the Committee:

Thank you for this opportunity to testify today on Supply Chain Security, Global Competitiveness, and 5G.

The National Telecommunications and Information Administration (NTIA) in the Department of Commerce is responsible for advising the President on telecommunications and information policy. NTIA's programs and policymaking focus on a broad range of issues that include spectrum management and availability, broadband connectivity, and the growth and stability of the Internet. NTIA also is the agency charged with oversight of FirstNet, the independent authority within NTIA that is tasked with ensuring the development, building, and operating of the nationwide broadband network that equips first responders with essential digital tools that help save lives and protect U.S. communities.

During a time when an ever-changing landscape of services, technologies, and global industries are seeking to shape the development and deployment of 5G networks, NTIA collaborates with other Commerce bureaus and Executive Branch agencies to develop and advocate for domestic and international policies that preserve the open Internet and advance key U.S. interests. NTIA coordinates Executive Branch communications activities and represents the Administration's policies before the Federal Communications Commission (FCC).

The Nation's telecommunications infrastructure is the physical medium through which all Internet traffic flows. It underpins the foundation of our digital economy. NTIA's role is to foster national safety and security, economic prosperity, and the delivery of critical public services through telecommunications. In this capacity, NTIA is involved in numerous policy issues that affect the security of critical elements of our Nation's telecommunications infrastructure.

Our support includes working with our interagency partners to enhance the security of our Nation's telecommunications supply chain, advocating the United States' longstanding policy against data localization regimes, and participating in Executive Branch reviews of applications before the FCC that involve transactions with a significant foreign ownership component. We also are assisting the Secretary of Commerce, as needed, on the implementation of the Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

Managing U.S. Spectrum Resources

The United States is dependent on reliable access to the finite resource that is radiofrequency spectrum. The Federal government is the most sophisticated consumer of spectrum in the world. Our armed forces, law enforcement agencies, scientists, and engineers all rely on spectrum to successfully serve the public. By protecting critical spectrum resources, we ensure that our military remains strong and our scientific understanding remains second to none.

At the same time, our technology industries lead the world in putting spectrum to use in innovative ways that bring massive economic and societal benefits to Americans. These range from powering the connectivity of the smart devices in our hands to the satellites circling in our skies.

In our competitive world, our country does not have the luxury of pursuing only some of our national priorities. We must pursue and achieve all of them, which will require the ingenuity and close coordination between NTIA and all of our federal partners as well as the private-sector.

As with any critical resource, access to spectrum must be managed efficiently and effectively in order to provide additional spectrum for wireless 5G spectrum access while ensuring federal agencies have sufficient spectrum to complete their missions. As management of spectrum licenses or authorizations becomes more automated and networked, the security of the information systems utilized becomes even more essential and NTIA will work to ensure that it continues to manage risk to these essential systems.

The Administration views spectrum resources as a strategic asset for our economy and our national security. This means we must take a comprehensive, whole-of-government view on how to use spectrum and how to best unleash the power of spectrum-based technologies for the private sector. To accomplish this, we must follow several major principles.

The first of these is balance. We must balance the competing needs of all major equities to reach all of our national goals. For example, the Department of Defense is already devoting resources to adopt 5G technologies for national security and private sector satellite technologies that are interdependent with federal operations.

The second principle is to think long-term and comprehensively. We must develop an over-arching framework that will address new spectrum demands not just for today, but for the century to come.

The third principle is to be innovative and pioneering. This requires us to think beyond the traditional model of one allocation for one licensee for one use.

In October 2018, President Trump signed the "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future." The memorandum set forth a "balanced, forward-looking, flexible, and sustainable approach to spectrum management" including the development of a new National Spectrum Strategy. To develop this Strategy, NTIA has worked with the Secretary's office, federal agencies, and the White House to detail a path for realizing the President's vision of a long-term spectrum infrastructure that sustains American technological dominance. As called for in the memorandum, federal agencies also identified their current spectrum usage and defined their anticipated future needs over the next 15 years.

Securing the Snpply Chain

The telecommunications infrastructure is critical to nearly every aspect of the American economy and national security. The complex global telecommunications supply chain is increasingly vulnerable due to the proliferation of some foreign-sourced products and services. One way NTIA helps address these challenges is by supporting the Secretary of Commerce in implementing the President's Executive Order on Securing the Information and Communications Technology and Service Supply Chain.

NTIA also serves as a member of the executive committee of DHS's Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, which provides advice and recommendations to DHS and private sector owners and operators of ICT critical infrastructure about how to assess and manage risks associated with the ICT supply

chain. Finally, NTIA strongly supports the recently updated version 1.1 of the NIST Cybersecurity Framework, which incorporates a new section helping organizations understand and manage supply chain risks.

The Department of Commerce is a member of the Federal Acquisition Security Council, which was established by the SECURE Technology Act. The council formalized aspects of several interagency efforts in which NTIA has participated, including the Supply Chain Risk Management Information Sharing Working Group led by the Director of National Intelligence; and the Section 889 Working Group, led by DHS and GSA. The Commerce representative to the Council brings economic impact analysis to bear related to the information and communications technology sector, identifies risks and unintended consequences of proposed actions, and explains communications sector incentive and market structures.

As a contributor to these efforts, NTIA has provided telecommunications subject matter expertise, as well as insight into cybersecurity vulnerability coordination and detection, the Internet of Things and next generation network security, and software component transparency, a critical component for minimizing, detecting, and mitigating supply chain risk.

FirstNet Resilience and Reliability

Congress created the First Responder Network Authority (FirstNet) in the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, 126 Stat. 201 (2012), with the duty to ensure the deployment, operation, and maintenance of the nationwide public safety broadband network (FirstNet network), to address the lack of a standardized interoperable communications platform for first responders. The critical nature of first responders' communications demands that the network must be resilient and provide high availability, security, and privacy protections.

Cybersecurity is critical to the FirstNet mission to ensure all components of the FirstNet network are secure, reliable, and work together to provide first responders the data and communications they need on time, intact, and secure. From its inception, the FirstNet network has incorporated end-to-end cybersecurity for the network and its users. In partnering with AT&T, FirstNet invested years of planning and experience to create a secure environment for first responders. Among the key components of the enhanced cybersecurity of the FirstNet network design is the nationwide dedicated core network implemented by AT&T.

FirstNet network subscriber traffic running through the dedicated core ensures higher levels of reliability, redundancy, and protection through the dedicated processing and routing of the public safety traffic. Another critical enhancement can be found in the dedicated Security Operations Center (SOC), which handles continuous monitoring, detection, and mitigation efforts in cybersecurity for the network. The SOC provides 24/7/365 coverage and support for all cybersecurity considerations and is backed up by the full global network visibility of AT&T to ensure proactive protection for public safety.

From a cross-functional perspective, all aspects of cybersecurity are evaluated and reviewed within the context of the FirstNet network. This includes user equipment, such as phones, tablets, and in-vehicle routers, and anything that is connected to the network (i.e., the Internet of Things (IoT)). Similarly, there are processes in place for the vetting and inclusion of software applications developed for the public safety market.

Government and Industry Collaboration

To manage and address the risks posed by 5G, the U.S. government is taking an interagency approach to this issue, led by the Director of the National Economic Council (NEC) at the White House. The National Security Council (NSC) Cybersecurity Directorate and the NEC co-lead a regular 5G interagency Policy Coordination Committee through the National Security Presidential Memorandum - 4 process. These meetings are an opportunity to discuss and come to decisions on key 5G issues, such as work underway in standards bodies, as well as to provide updates on interagency 5G activities.

NTIA collaborates across the U.S. government and industry on numerous additional efforts related to the security of the nation's Internet architecture. We also have been working closely with the NSC staff and our interagency colleagues on implementing the National Cyber Strategy, which just marked its one-year anniversary. In that effort, we shared our activities across the interagency and looked for synergies to maximize the impact of the strategy. NTIA will continue to participate in these efforts.

3rd Generation Partnership Project

NTIA is a regular participant in the 3rd Generation Partnership Project (3GPP), which unites seven telecommunications standards development organizations from across the world and provides their members with a stable environment to produce the reports and specifications that define the 3GPP technologies behind today's ubiquitous mobile wireless networks and the emergence of 5G. 3GPP addresses cellular technologies, including radio access, security, core network and service capabilities that provide a complete system description for mobile telecommunications.

Cybersecurity Multistakeholder Processes

NTIA's cybersecurity multistakeholder processes contribute to the security of the nation's Internet architecture. Our ultimate objective is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions. We think this kind of work can form the foundation of broader security baselines.

Most recently, NTIA has been working on software component transparency. Most modern software is not written completely from scratch, but includes existing components, modules, and libraries from the open source and commercial software world, which can be challenging to track. The IoT compounds this phenomenon, as new organizations, enterprises and innovators take on the role of software developer to add "smart" features or connectivity to their products. The sheer quantity of software inputs means that some products ship with vulnerable or out-of-date components.

NTIA convened a multistakeholder process late last year between software vendors and the enterprise customer communities who use these products. Stakeholders have talked to industry and government experts across the supply chain to capture their perspectives on how a software bill of materials, or "SBOM," is helping them today, and what they could do in the future if this practice became more widespread. We are working toward a shared vision of what the "minimum viable" implementation looks like, and how it can be implemented across the supply chain.

Botnet Coordination

Another example of NTIA's contribution to the protection of the Internet infrastructure is our work with NIST and DHS on the Botnet Report, and subsequent road map. Botnet attacks can have large and damaging effects, and they put the broader network at risk. The usual distributed denial of service (DDoS) mitigation techniques, including network providers building in excess capacity to absorb the effects, are designed to protect against botnets of a certain size. But much bigger botnets now capitalize on the sheer number of Internet of Things (IoT) devices.

The Botnet Report outlines a positive vision for the future, cemented by six principal themes and five complementary goals that would improve the resilience of the Internet ecosystem. For each goal, the report suggests supporting actions that can be taken by both government and the private sector. The Departments of Commerce and Homeland Security developed the report through an open and transparent process for the specific purpose of identifying stakeholder actions as opposed to government regulations. One of the report's focus areas was edge devices, including the components that go into them. Modern development techniques rely on a combination of open source and commercially available components. To meet future security demands, such components must be traceable through the supply chain and offer greater assurance.

Remediating botnet threats is an ecosystem-wide challenge that will take time to accomplish – we recognize that botnets are not going to be "solved" in one year. At the end of this year, the Departments of Commerce and Homeland Security will provide a status update to the President that reviews progress, tracks the impact of the road map and sets further priorities.

Conclusion

Deploying robust and secure 5G networks across the country will enable life-changing and life-saving advances from smart communities to the Internet of Things as well as technologies that will help to save lives and enhance our national security. The U.S. wireless industry has invested billions of dollars toward the development and deployment of new, powerful 5G networks.

However, the United States will only be able to harness the true economic and national security benefits of these networks if they are secure. NTIA is committed to coordinating across the Federal Government and engaging with the private sector to ensure this is the case. Thus, NTIA—and the Department of Commerce more broadly—are taking powerful steps to advance this technology to ensure the security of these networks and that the United States leads the world in 5G. We are focused on policies that will increase the amount of spectrum available for 5G, secure the supply chain, remove roadblocks to spur even greater investment in 5G, help make networks more secure and resilient against cyberattacks. Additionally, we support U.S. industry in global standards development as well as conduct and coordinate targeted research activities.

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

Prepared Statement of:
Robert L. Strayer
Deputy Assistant Secretary of State for
Cyber and International Communications and Information Policy

Hearing before the:
Senate Committee on Homeland Security and Governmental Affairs
on
Supply Chain Security, Global Competitiveness, and 5G

October 31, 2019

Chairman Johnson, Ranking Member Peters, and members of the Committee, thank you for today's opportunity to testify.

As the world becomes more interconnected, the security of our information communications technology (ICT), including the fifth generation of wireless technology (5G), is becoming increasingly important for our national security and economic prosperity, as well as the protection of human rights globally. The Department of State, under Secretary Pompeo's leadership, is in charge of the United States' international engagement on ICT security and our campaign to convince our allies and partners of the importance of 5G security.

Our mission is to engage our allies and partners to advance our shared vision for an open, interoperable, reliable, and secure digital environment, including for 5G.

5G will be transformative, as it will provide consumers and businesses with speeds up to 100 times faster than 4G, delay times of less than a millisecond, and networks capable of handling millions of new devices.

These advantages will empower a vast array of new critical services – from autonomous vehicles and transportation systems, to telemedicine, to automated manufacturing and traditional critical infrastructure, such as electricity distribution. The massive amounts of data transmitted by devices on 5G networks will also advance artificial intelligence.

With all these services relying on 5G networks, the stakes for safeguarding these vital networks exponentially increases.

As countries around the world upgrade their communications systems to 5G technology, we are urging them to adopt a risk-based security framework. To this end, the Department is executing a global campaign on 5G security that includes strategic bilateral and multilateral engagements to convince our allies and partners of the importance of adequately securing these networks.

An important element of this risk-based security approach is a careful evaluation of hardware and software equipment vendors and the supply chain. The evaluation criteria should include the extent to which vendors are subject to control by a foreign government with no meaningful checks and balances on its power to compel cooperation of these vendors with its intelligence and security agencies. While this should apply to vendors from all countries, our current concern is primarily with equipment vendors from the People's Republic of China (PRC) for multiple reasons.

Our assessment of the problem is that the PRC could compel Chinese equipment vendors to act against the interests of U.S. citizens and citizens of other countries around the world. If allowed to construct and service 5G networks, Chinese equipment vendors will have access to critical networks and understanding of network vulnerabilities. This information could be exploited, as outlined in China's National Intelligence Law, for the Chinese Communist Party to disrupt critical infrastructure, intercept sensitive transmissions, and acquire sensitive technology and intellectual property.

Specifically, the National Intelligence Law compels Chinese citizens and organizations to cooperate with Chinese intelligence and security services and to keep such cooperation secret.

In addition, the Chinese Communist Party does not have any meaningful checks or balances on its powers. As President Xi Jinping told security officials in January, China does not walk the "Western road" of constitutionalism, separation of powers, or judicial independence.

Chinese technology firms are already working with authoritarian regimes – often hand-in-hand with the Chinese government – to suppress freedom of expression and other human rights through arbitrary surveillance, censorship, and targeted restrictions on Internet access. If Chinese companies build the underlying 5G infrastructure, they will be in an even better position to facilitate these activities.

Moreover, the PRC and Chinese firms have a long history of intellectual property theft to benefit its interests. In December 2018, the United States announced that since at least 2014, Chinese cyber actors associated with the Chinese Ministry of State Security hacked multiple U.S. and global managed service and cloud providers. These cyber intrusions allowed the PRC to compromise the networks of the providers' clients, including global companies located in at least 12 countries. Countries must not allow 5G to be another vector for the PRC to steal their intellectual property.

Furthermore, Chinese companies, such as Huawei have benefited from subsidized financing and currency manipulation for their equipment sales. Countries should adopt the best practices in procurement, investment, and contracting, and require that financing be commercially reasonable, conducted openly and transparently, and based on free market competition, while taking into account trade obligations.

To manage and address the risks posed by 5G, the entire U.S. government is taking an interagency approach to this issue, led by the Director of the National Economic Council at the White House. The National Security Council (NSC) Cybersecurity Directorate and the National Economic Council co-lead a regular 5G interagency Policy Coordination Committee (PCC) through the National Security Presidential Memoranda (NSPM) - 4 process. These meetings are an opportunity to discuss and come to decisions on key 5G issues, such as participation in standards bodies, as well as to provide updates on interagency 5G activities. The Department of State is mobilized to continue its bilateral and multilateral engagements and to coordinate with its interagency partners.

That said, the United States is a leader in 5G deployment, and we will do so using trusted vendors to build our networks. Through our engagements, many other countries are now acknowledging the supply chain risk and beginning to strengthen their information and communications technology security alongside the United States.

For example, in August 2018, Australia issued 5G security guidance to Australian carriers to protect their networks from unauthorized access or interference by "vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law."

Japan has also taken measures to address supply chain risks using existing and new authorities. Most recently, in April, Japan announced spectrum awards conditional on 12 criteria, including one on network security that requires operators to "take appropriate cyber security measures including measures to respond to supply chain risks."

Likewise, Taiwan had previously adopted measures to protect 4G networks from untrusted equipment vendors and has extended these measures to protect all 5G government networks and critical infrastructure.

In May, the Czech Republic hosted more than 140 representatives of 32 countries from around the world, as well as the European Union and NATO, to build consensus on a common approach to 5G security. This effort produced the Prague Proposals -- a set of recommendations on how to build secure and resilient 5G networks based on free and fair competition, transparency, and the rule of law.

We have been working to advance the principles envisioned in the Prague Proposals by encouraging other countries to endorse the Proposals and by signing joint declarations or memorandums of understanding on 5G security with like-minded countries, including Romania and Poland.

Most recently, the European Commission and member states released their coordinated risk assessment of 5G security. We welcomed the assessment and how it clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances in place.

The assessment also highlighted the corporate ownership structure of 5G suppliers as a potential risk factor, which aligns with the U.S. assessment and the Prague Proposals' call for transparency.

In addition, the assessment recognized that the "edge" and "core" of networks will blur in 5G networks, requiring increased security measures be applied to all parts of the network. This aligns with the U.S. assessment that you cannot mitigate the risk of untrusted suppliers by limiting them to certain parts of a network. Untrusted suppliers anywhere in the network could be exploited by authoritarian governments for espionage, traffic disruption, data manipulation, and/or theft of sensitive information and intellectual property.

The EU risk assessment itself is a sign of progress in our 5G campaign as it demonstrates that our allies and partners are recognizing the risk of untrusted vendors, but our work is far from over.

Next, the European Commission and member states will use this assessment to develop and agree upon "a toolbox of possible risk mitigating measures" by the end of the year. This toolbox will outline specific, albeit non-binding, actions that member states can take to secure their 5G networks. It is important that this toolbox address the vulnerabilities and risks identified in the EU's risk assessment, including from untrusted suppliers, and that member states then implement binding national measures to safeguard their networks.

Thank you for the opportunity to appear before the Committee today. I look forward to your questions.

STATEMENT OF
JESSICA ROSENWORCEL
COMMISSIONER
FEDERAL COMMUNICATIONS COMMISSION
BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
WASHINGTON, D.C.
OCTOBER 31, 2019

Good morning, Chairman Johnson, Ranking Member Peters, and Members of the Committee. Thank you for the opportunity to appear before you today.

For the last decade, the United States has led the world in wireless technology and performance, and we have reaped the benefits. The smartphone revolution began here on our shores. The new world of wireless it fostered fueled economic growth at home and abroad. It helped secure our global dominance in the technology sector.

Let me be blunt. That authority is now being challenged. Extending this leadership into the next generation of wireless technologies—5G—is going to be difficult. But it's worth the effort. With speeds as much as 100 times faster than present networks and much lower latency, these networks will kickstart the next big digital transformation. By connecting many more things in many more places, 5G offers new ways to foster economic activity and improve health, education, the environment, and more. In short order, the smartphone could become the least innovative thing about our wireless world.

However, earlier this year the Defense Innovation Board—the United States military's premier advisory board of academic researchers and private sector technologists—surveyed the state of next-generation 5G networks and issued a sober warning. They found that "the country that owns 5G will own innovations and set the standards for the rest of the world," and "that country is currently not likely to be the United States."

This is a clarion call. Other nations saw very clearly the success in the United States with the last generation of wireless technology and are working overtime to ensure that they secure a leadership position—and their efforts are bearing fruit.

We see it in deployment. Switzerland has more commercial 5G deployments than any other country. South Korea has led the world in bringing a mix of high-band and mid-band spectrum to auction to support 5G service. China, Germany, and Japan have built out more infrastructure on a per capita basis to carry 5G airwaves.

We see it in activity in standards bodies. Countries are amassing bigger delegations and submitting more proposals at international fora, like 3GPP and the International Telecommunication Union, where 5G specifications are being hammered out.

We see it in patents and equipment. Based on recent reports, Chinese companies own 36 percent of all 5G standard-essential patents—more than double their share of 4G patents—setting themselves up for big royalties ahead. Companies in the United States today, by contrast, hold just 14 percent. In fact, there are no longer any United States-based manufacturers of key 5G network equipment.

The truth is we are facing well-resourced challenges to our 5G leadership from every direction. And so far, we do not have a comprehensive national plan in place with a fully coordinated interagency response to meet that challenge.

We need one—and here are four ideas it should include.

First, if we want to lead in 5G, we have to secure the 5G supply chain. The underlying truth about next-generation communications networks in many parts of the world is that technology developed in China will be at the center. This threatens to expose our networks and our most private data to undue foreign influence.

The good news is we are making some progress with our federal networks. The Pentagon has banned the sale of insecure Chinese equipment on military bases. In addition, the National Defense Authorization Act prohibits federal agencies from using this equipment. But when it comes to our commercial networks, we are still woefully behind. At the Federal Communications Commission we have a rulemaking to ensure that our universal service fund, which provides billions annually to support broadband deployment in rural communities, going forward will not be used to purchase insecure network equipment. That rulemaking has inexplicably stalled for more than a year and a half. But now, perhaps because you announced this hearing, we have publicized that we will vote on this in three short weeks.

Second, we need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far because no network stands by itself. Our networks still will connect to insecure equipment abroad. So we need to start researching how we can build networks that can withstand connection to equipment vulnerabilities around the world. One way to do this is to invest in virtualizing radio access networks—or open RAN. The RAN is the most expensive and restrictive part of the network—it sits between your device and a carrier's core network. Today, all major components of a RAN have to come from the same vendor. There is no way to mix and match. But if we can unlock the RAN and diversify the equipment in this part of our networks, we can increase security and push the market for equipment to where the United States is strongest—in software and semiconductors. This also will give carriers around the world that are locked into upgrade cycles with a single foreign vendor a way out.

Third, we need smarter spectrum policy. To date, the FCC has aggressively focused its early efforts to support 5G wireless service by bringing only high-band spectrum to market. This is a mistake. The rest of the world does not have this singular early focus on high-band, millimeter airwaves, with good reason. These airwaves have substantial capacity but their signals do not travel far and are easily blocked by walls. As a result, commercializing them is costly—especially in rural areas. The sheer volume of antenna facilities required to make this

service viable will limit deployment to the most populated urban areas. This means our early 5G spectrum policy could create 5G haves and have-nots, deepening the digital divide that already plagues too many rural communities nationwide. That's not right. If you care about rural broadband, this matters. The FCC needs to change course and make it a priority to auction mid-band spectrum, which has a mix of capacity and propagation which is better suited to extend the promise of 5G wireless service to everyone, everywhere in the country.

Fourth and finally, with 5G we are moving to a world with billions of connected devices around us in the internet of things. We need to adjust our policies now to ensure this future is secure. After all, the equipment that *connects* to our networks is just as consequential for security as the equipment that goes *into* our networks.

Here is what that could look like. Every device that emits radiofrequency at some point passes through the FCC. If you want proof, pull out your smartphone or take a look at the back of any computer or television. You'll see an identification number from the FCC. It's a stamp of approval. It means the device complies with FCC rules and policy objectives before it is marketed or imported into the United States. This routine authorization process takes place behind the scenes. But the FCC needs to revisit this process and explore how it can be used to encourage device manufacturers to build security into new products. To do this, we could build on the National Institutes of Standards and Technology draft set of security recommendations for devices in the internet of things. This effort specifies the cybersecurity features to include in network-capable devices, whether designed for the home, hospital, or factory floor. It covers everything from device identification, device configuration, data protection, access to interfaces, and critical software updates. In other words, it's a great place to start—and we should do it now.

Chairman Johnson, Ranking Member Peters, and Members of the Committee, thank you once again for holding this hearing. Thank you for providing me with the opportunity to offer my views. I look forward to answering any questions you have.

November 8, 2019

Hon. Ron Johnson
Chairman
Senate Committee on Homeland Security &
Governmental Affairs
328 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Johnson:

As the Executive Vice President, Advocacy & Government Relations of the C-Band Alliance (CBA), I commend you for raising important concerns in the Committee's October 31, 2019 hearing, *Supply Chain Security, Global Competitiveness, and 5G*, regarding the need to eliminate bureaucratic roadblocks and incentivize private telecommunications companies to deploy 5G networks so that the United States can defeat China in the global race to 5G.

Time is of the essence. Just last week, the three largest Chinese mobile network operators—China Telecom, China Unicom, and China Mobile—simultaneously announced the rollout of their 5G networks and launched their long-awaited 5G service plans in dozens of cities across China. As you and other members of the Committee accurately recognized, losing the global race to 5G to China would bring dire economic and national security consequences and give China the power to unilaterally establish the technological rules of the road for decades to come.

The CBA agrees that the United States needs to act as quickly as possible to maintain its 5G leadership, and that is why the CBA is taking the lead to help repurpose a valuable portion of mid-band spectrum for 5G known as the C-band.

The Federal Communications Commission (FCC) has initiated a rulemaking proceeding on how best to accelerate 5G deployment by freeing up the C-band for mobile use. Over the last year, the C-band satellite operators that comprise the CBA have taken extraordinary efforts to help repurpose this spectrum for 5G while meeting the government's twin goals of speed and security.

Under the CBA's approach, its fixed satellite service member companies will voluntarily relinquish their non-interference rights and undertake the clearing of a substantial portion of C-band spectrum for next-generation 5G terrestrial services. The satellite operators will then relocate their services to the upper portion of the C-band and continue to transmit video and radio content to cable programmers, broadcasters, and local television and radio stations across the continental United States. Never before have spectrum holders proposed to the Commission to voluntarily relinquish a substantial portion of their licensed spectrum; to cover the costs of clearing the spectrum; and to protect the important services upon which hundreds of millions of Americans rely.

The CBA's consensus proposal has won widespread support from public interest think tanks,[1] wireless carriers,[2] the satellite industry,[3] content distributors,[4] broadcasters,[5] empirical economists,[6] equipment manufacturers,[7] and aerospace companies.[8]

---

[1] *See, e.g.*, Letter from American Consumer Institute, American Enterprise Institute, Competitive Enterprise Institute, Heritage Action for America, Lincoln Network, and R Street Institute, to Reps. Walden and Latta (Oct. 29, 2019); Letter from Grover Norquist, President, Americans for Tax Reform, to Communications & Technology Subcommittee, U.S. House Committee on Energy & Commerce (Oct. 28, 2019); Comments of ITIF, GN Docket No. 18-122 *et al.*, at 1-2 (filed Oct. 29, 2018); Ex Parte Letter from Joe Kane, Technology Policy Fellow, R Street Institute, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 18-122 (filed Apr. 30, 2019).

The CBA's proposal enjoys such broad support because it will bring mid-band spectrum to U.S. wireless carriers in the fastest possible timeframe. If the FCC were to adopt the CBA's proposal by December 2019, the CBA would conduct an auction in the first half of 2020. The CBA would clear 300 megahertz for terrestrial 5G within 36 months of the C-band auction and clear 120 megahertz of spectrum in the 46 top metropolitan zones within 18 months of a final FCC order. With spectrum assignments occurring so rapidly, U.S. wireless carriers and technology vendors would have the certainty they need to plan their networks and make substantial investments in 5G equipment. These investments by leading U.S. carriers, in turn, will greatly promote the vendors of secure 5G equipment.

The CBA's approach is the fastest proposal before the FCC because it creates a financial incentive for CBA members to expedite the costly, complicated, and difficult voluntary clearing process and ensure that spectrum is repurposed where and when that would be efficient. Indeed, any economic benefit that CBA members realize will be a direct reflection of the economic value created by their entrepreneurial efforts to move scarce spectrum to a higher valued use.

In short, the CBA's proposal is the best plan to help bring the C-band most quickly to market and help win the global race to 5G while protecting the video and radio transmission services upon which hundreds of millions of Americans currently rely. More information about the CBA's proposal appears below, and I would be happy to answer any questions you may have. Thank you.

* * *

---

[2] *See, e.g.*, Ex Parte Letter from Gregory M. Romano, Vice President of Federal Regulatory and Legal Affairs, Verizon, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 18-122 (filed Oct. 9, 2019).

[3] *See, e.g.*, Comments of the Satellite Industry Association, GN Docket No. 18-122 *et al.* (filed Oct. 29, 2018).

[4] *See, e.g.*, Comments of the Content Companies, GN Docket No. 18-122, at 1-2 (filed Aug. 7, 2019).

[5] *See, e.g.*, Joint Reply Comments of the ABC Television Affiliates Association, CBS Television Network Affiliates Association, FBC Television Affiliates Association, and NBC Television Affiliates, GN Docket No. 18-122, at 4 (filed Aug. 14, 2019).

[6] *See, e.g.*, Will Rinehart, *Analyzing Plans To Reallocate C-Band for 5G Deployment*, American Action Forum (Oct. 7, 2019), https://bit.ly/32pODXn; T. Randolph Beard, George S. Ford, and Michael Stern, *Innovation in Spectrum Repurposing: The C-Band as a Principal-Agent Problem*, The Phoenix Center for Advanced Legal and Economic Public Policy Studies, at 3 (Sept. 2019), https://bit.ly/2kRqX42; Randolph J. May and Gregory J. Vogt, *A Free Market Approach Should Be Used to Reallocate C-Band Spectrum*, Free State Foundation, at 2 (July 17, 2019), https://bit.ly/2B7Yt3K; Reply Declaration of Jeffrey A. Eisenach, Ph.D., at 16, attached to Reply Comments of the C-Band Alliance, GN Docket No. 18-122 *et al.* (filed Dec. 7, 2018); Coleman Bazelon, *Maximizing the Value of the C-Band: Comments on the FCC's NPRM to Transition C-Band Spectrum to Terrestrial Uses*, Brattle Group, at 27, attached as App. A to the Joint Comments of Intel Corp., Intelsat License LLC and SES Americom, Inc., GN Docket No. 18-122 *et al.* (filed Oct. 29, 2018) ("*Maximizing the Value of the C-Band: Comments on the FCC's NPRM to Transition C-Band Spectrum to Terrestrial Uses*").

[7] *See, e.g.*, Reply Comments of Nokia, GN Docket No. 18-122 *et al.*, at 1 (filed Dec. 11, 2018).

[8] *See, e.g.*, Reply Comments of the Boeing Company, GN Docket No. 18-122 *et al.*, at 1 (filed Dec. 11, 2018).

Background

The global race to 5G is on and the United States is at great risk of falling behind. As countries compete with each other to move beyond the 4G networks of today, the United States must act quickly to ensure leadership in 5G technology.

The Department of Defense's Defense Innovation Board reported that "First-mover advantage will likely drive significant increases in [China's] handset and telecom equipment vendors market along with their domestic semiconductor and system suppliers. . . . China's handset and internet applications and services are likely to become dominant, even if they are excluded from the US. China is on a track to repeat in 5G what happened with the United States in 4G." U.S. leadership in 4G laid the foundation for what are now some of the most well-known companies and brands in the world—Uber, Instagram, and Snapchat, to name a few. Wireless industry association CTIA reported that "U.S. leadership in 4G accounted for nearly $100 billion of the increase in annual GDP by 2016 as the trajectory of the wireless industry's contribution to US GDP shifted from a projected $350.3 billion in 2016 to a realized $445.0 billion."

The benefits of 5G are likely to dwarf those of 4G. 5G promises speeds up to twenty times faster than 4G, and it is expected to bring an incremental $500 billion to the U.S. GDP, drive $275 billion in investment, and create 3 million jobs. Dubbed the "network of networks," 5G will enable smart technologies and the Internet of Things (IoT) that will result in new levels of automation and create entirely new industries. Autonomous cars, smart communities, the industrial Internet of Things, immersive education, telemedicine, and other cutting-edge innovations will be possible with 5G. As the number of IoT devices continues to grow, potentially totaling 31 billion connected devices worldwide by 2020, the limits to what IoT technology can do may be defined not by the devices, and certainly not by engineers' imaginations, but by the network that supports them and the bandwidth available. Meanwhile, 5G promises to close the digital divide by giving rural communities a meaningful alternative to fixed broadband services.

Rapidly transitioning our telecommunications networks to 5G therefore remains a national imperative. Some economists have calculated that for each year the rollout of 5G is delayed, the U.S. economy would lose $50 billion in GDP.[9] Moving to 5G quickly also ensures that the United States remains relevant in the development of all of the equipment, applications, and services that will run over 5G. If we are late to the party, companies in other nations will establish the technology and therefore the standards for devices and applications that run on 5G. This time advantage will be the determining factor for 5G winners and losers.

The Mid-Band Opportunity

Wireless spectrum bands have different characteristics depending on the frequency used. Higher frequency spectrum can carry more data, but it travels shorter distances, requires more antennas, and is more susceptible to interference from rain, foliage, and other physical barriers. Lower frequency spectrum, by contrast, can travel great distances, but it cannot carry as much data.

Mid-band spectrum is the "Goldilocks" band for 5G, with the right balance of coverage and capacity to facilitate 5G adoption throughout urban, suburban, and rural America. In particular, the 3.7-4.2

[9] Roslyn Layton, *For mid-band spectrum, markets can produce better outcomes than regulators can engineer*, American Enterprise Institute (July 26, 2019), https://bit.ly/2NiYCZr ("[A] public auction would reportedly take seven to 10 years to complete, with each year representing a missed revenue opportunity of some $50 billion.").

GHz band—known as the C-band—can deliver the high-throughput, low-latency performance that next-generation mobile networks demand. The C-band, in other words, is ideally suited for 5G.

Clearing mid-band spectrum for 5G with a market-based approach will speed economic growth, generating tax receipts, jobs, and other societal benefits years faster than any alternative. For example, the CBA has committed to making a significant contribution to the U.S. Treasury. And the speed provided by a market-based approach produces gains to consumers and American businesses. Economist Coleman Bazelon calculated that one year of delay in clearing the C-band could reduce the total social value of repurposing the spectrum by between 7 percent and 11 percent and every $1 billion in delay costs would create total social costs of up to $20 billion.[10]

Two problems, however, complicate repurposing a portion of the C-band for 5G. First, the C-band forms the backbone for the delivery of video and radio programming that reaches nearly 120 million U.S. households. The C-band also supports government and public safety operations, provides critical links to remote and underserved areas, and ensures communications systems' availability during disasters when terrestrial services fail. And the spectrum band immediately above 3.7-4.2 GHz supports aeronautical services, which need additional protection from terrestrial mobile operations.

Second, each of the operating satellite companies have a non-exclusive right to use the entire C-band over the entire continental United States. This policy means that no one satellite operator alone can relinquish the full rights to the C-band in any specific portion of the United States. Therefore, to encourage and enable an efficient transition of spectrum to 5G, there must be a voluntary agreement among the satellite operators that provide C-band service in the U.S., a process to incentivize them to manage their transition, and safeguards for existing C-band users.

The CBA's members are heavily invested in the C-band. In 2001, Intelsat paid $1.0 billion for certain U.S. satellites of Loral, and in 2006, Intelsat paid $3.2 billion when it bought PanAmSat; similarly, SES paid $5 billion in 2001 when it bought GE Americom. Since then, CBA members have made significant investments in the C-band, having built a substantial U.S.-centric network infrastructure, sales force, customer base, and related U.S. revenues based on a replacement expectancy. It would be unreasonable to expect incumbents to willingly—much less quickly—surrender or transfer spectrum that they are actively using to deliver contracted services—now and in the future—for the benefit of their customers and shareholders.

CBA's Solution

To solve these challenges, the four satellite companies providing C-band services in the continental United States formed a consortium called the C-Band Alliance. On October 28, 2019 the CBA announced that it developed a plan with C-band customers to clear and relinquish the lower 300 megahertz of the C-band—60 percent of its spectrum, inclusive of a 20 megahertz guard band—for terrestrial 5G within 36 months of the C-band auction. This amount represents a major increase over the CBA's previous proposal to clear 200 megahertz of spectrum. The CBA will clear 120 megahertz of spectrum (inclusive of a 20 megahertz guard band) in the 46 top metropolitan zones within 18 months of a final FCC order.

The member companies of the CBA have been working with their customers to ensure that sufficient C-band spectrum remains available for continued content distribution, while maximizing the portion repurposed for terrestrial 5G use. These cooperative efforts have been fruitful, and have led the

[10] *Maximizing the Value of the C-Band: Comments on the FCC's NPRM to Transition C-Band Spectrum to Terrestrial Uses* at 27.

CBA, with the support of C-band customers, to propose making 280 megahertz of spectrum available for terrestrial 5G use via its market-based approach, as well as a 20 megahertz guard band to protect on-going operations in the band. The customer signatories represent key players in the current content distribution ecosystem upon which nearly 120 million American households rely.

This increase in the amount of spectrum proposed by the CBA to be cleared for 5G use is made possible, in part, by the cooperation of C-band customers and the planned implementation of technologies such as advanced video compression—including High Efficiency Video Coding ("HEVC")—advanced modulation, and single format transport. Each of these technologies improves the efficiency of satellite video delivery, allowing the same video content to be transmitted over less spectrum. A number of video content distributors have already adopted or are in the process of adopting these technologies, including HEVC. The CBA's market-based plan makes it economically viable for others to also enjoy the benefits of these technology upgrades because the CBA will pay the costs incurred by the Customer Signatories and others adopting such technologies to clear spectrum.

Importantly, the CBA is committed to ensuring that C-band and other satellite operator customers enjoy continued access to 200 megahertz of C-band satellite spectrum in an interference-free environment before, during, and after the transition of 280 megahertz (plus a 20 megahertz guard band) of C-band spectrum to 5G. The CBA's proposal is the only proposal before the FCC that protects existing satellite services while solving the holdout problem. And the CBA's proposal frees up 5G spectrum for immediate deployment much faster than any alternative offered to date.

Protects Existing Satellite Services

Although the C-band is well-suited for commercial deployment of 5G, that spectrum was assigned decades ago to satellite companies that today deliver virtually all of the television and radio programming consumed by U.S. citizens, powering more than $100 billion in annual broadcast business.

Four satellite providers currently use C-band spectrum to broadcast video and radio content from cable programmers and broadcasters to cable companies' local distribution centers, as well as to local television and radio stations across the continental United States. More than 300 million Americans enjoy this video and radio content. All of the major television networks like FOX and NBC, all cable networks like ESPN and C-SPAN, and radio networks like NPR and religious broadcasters rely on C-band to get their programs to viewers and listeners. C-band spectrum is also used for telecommunications infrastructure, certain critical weather tracking services, and private video and data networks in the United States—all of which depend upon the highly reliable propagation characteristics of C-band spectrum.

Unless carefully managed, introducing mobile services into the C-band will interfere with the satellite transmissions carrying the TV and radio programming enjoyed by hundreds of millions of Americans. Proposed 5G services in the C-Band operate at a significantly higher power level than satellite services. With detailed knowledge of every television, radio, and data network in the U.S., the satellite operators understand the technical and operational necessities to accomplish such a transition in a seamless manner. Drawing upon the unique knowledge and capabilities of the satellite operators, the CBA's proposal is designed to streamline this extremely complex task. Under the CBA plan, 300 megahertz would be cleared by increasing existing transmission capacity through the procurement and launch of new satellites. Every existing customer will be kept whole: they will continue to distribute their programming and not incur the costs of the transition. Thus, the CBA plan protects every service that is currently provided over C-band in the United States.

No other plan under consideration guarantees existing broadcast and cable programmers the same high-quality, low-cost satellite distribution capability they have today. For example, some commentators with no experience distributing nationwide content have argued that fiber could be a suitable replacement for C-band spectrum. Not so. In reality, transitioning all C-band operations to fiber would be enormously complex and lack the reliability of C-band satellite distribution. And most importantly, most informed stakeholders in this proceeding understand that there is almost no possibility that the move to fiber could be completed in a 18-36 month timeframe. The time it will take to design a fiber network, obtain local permits, procure broadcast-quality architecture, mount the fiber, and install the components required to interconnect the fiber with 13,500 earth stations, 60 percent of which are rural, will take many years, if not an entire decade. Meanwhile, the total estimated 30-year costs for a massive fiber installation could be in the range of $20 billion to $30 billion or more. In short, a fiber-based proposal goes against the FCC's objective of moving as quickly as possible to allow 5G services in the band.

Solves the Holdout Problem

The primary reason market forces cannot repurpose the C-band on their own is due to what is known as the "holdout problem" that results from overlapping, non-exclusive rights to transmit in the band. Currently, satellite providers have rights to transmit across the entire 500 megahertz of the C-band to their customers and other users who receive signals from across the band. The problem created by these overlapping rights is that to reallocate any portion of the band at any specific location requires coordination of all relevant rights holders.

The CBA proposal solves the holdout problem, and it is the only proposal before the FCC that does so. First, it promotes coordination and collaboration by encouraging all C-band operators providing service in the continental United States to participate in the CBA and in the CBA's negotiations of agreements with prospective terrestrial mobile service providers. The CBA eliminates the need for a terrestrial mobile service provider to enter into multiple contracts with satellite operators for access to the spectrum, which would be time-consuming and inefficient.

Second, the CBA's proposal addresses the holdout problem by incentivizing each eligible C-band satellite operator to join the C-Band Alliance. All satellite operators affected by reallocation of the C-band and their relocation into a smaller portion of the band will be compensated for their costs. As an enticement to collaborate and participate in the process, eligible satellite operators that join the CBA will receive compensation for their prior investment and opportunity costs (in addition to compensation for their reconfiguration and relocation costs) based on objective and verifiable measures, such as their 2017 C-band satellite service revenues.

The CBA proposal solves the holdout problem even with Eutelsat's recent announcement regarding its membership in the CBA. Eutelsat has stated that it "continues to support the CBA's proposal of employing a secondary markets approach to rapidly clear a significant portion of the 3.7-4.2 GHz band for 5G wireless services," and Eutelsat's Chief Executive Officer has "clearly expressed his agreement to a significant contribution."[11] In fact, Eutelsat agrees with one of the most important principles of the CBA plan—namely, "the legitimacy of the CBA to act as the transition facilitator."[12]

---

[11] Ex Parte Letter from Bruce A. Olcott, Counsel, Eutelsat S.A., to Marlene H. Dortch, Secretary, FCC, GN Docket No. 18-122, at 1 (filed Sept. 19, 2019); Ex Parte Letter from Julie Burguburu, Group General Counsel, Eutelsat S.A., to Marlene H. Dortch, Secretary, FCC, GN Docket No. 18-122, at 1 (filed Oct. 3, 2019) ("Eutelsat Oct. 3 Letter").

[12] Eutelsat Oct. 3 Letter at 1.

The CBA's proposal is economically sound. As Nobel Laureate economist Ronald Coase observed many years ago, market forces will lead firms to organize themselves so as to internalize such transaction costs to achieve more efficient outcomes. That is exactly what the CBA does here. The CBA represents a solution to the nonexclusive right to use the C-band. Through the voluntary formation of the CBA consortium, uncooperative satellite providers will not benefit as much as cooperative ones. This brings the satellite operators under one umbrella, thereby creating an integrated entity with the ability and incentives to maximize efficiency and value creation for itself, and as a side benefit maximize efficiency and value creation for society.

Facilitates and Funds Expeditious Transition

The FCC has not conducted a traditional auction where incumbent licensees had shared and overlapping rights to use the spectrum. Typically when spectrum bands are repurposed through an FCC auction, the cost of transitioning geographically licensed incumbents is covered by new entrants. The overlapping, transcontinental transmission rights of the C-band satellite operators, however, mean that repurposing of the C-band cannot easily be done on a piece-meal basis. More complexity is added by the thousands of receive-only earth stations throughout the continental United States that must be protected. For example, co-frequency transmissions from wireless operators' base stations are likely to interfere with C-band earth stations 40 kilometers away, effectively requiring clearing well outside a mobile operator's license area.

For these reasons, repurposing a portion of the C-band is expected to cost billions to protect both incumbent earth stations and to ensure that C-band satellite operators retain enough capacity to deliver uninterrupted service during and after the transition. Under the CBA proposal, the members of the CBA, which have decades of experience protecting C-band users and delivering service with 99.999% availability, would facilitate the transition and ensure uninterrupted service for every C-band user. No other party has proposed a centralized mechanism to oversee and facilitate this transition.

It is not even clear how funding for a transition would be made available under alternative proposals. After an FCC auction, immediate funding would be needed to cover the billions of dollars of investments in many new satellites, customer hardware, filter technology, and filter installation in 30,000 to 35,000 earth station antennas across the U.S. Existing law, however, does not provide a funding source for these costs. FCC auction proceeds must be paid to the U.S. Treasury (with some limited exceptions). Therefore, winning bidders would likely need to directly negotiate and fund clearing with the multiple C-band satellite operators and thousands of earth stations. Under the CBA proposal, however, all of these costs are internalized and covered by the CBA.

Incorporates Transparency and Oversight

The CBA will hold a transparent auction of the C-band spectrum to all interested participants. This auction will be "public"—open to all bidders, large and small—and will look very similar to a traditional FCC auction. Under the CBA's proposal, moreover, the FCC will be involved every step of the way. We expect and invite FCC oversight of our auction process, which would be approved by the FCC before moving forward. Additionally, nothing about the proposed auction would change the process under which the FCC issues licenses for terrestrial mobile operation. The FCC possesses robust oversight authority over all licensing decisions, and must conduct full review and approve any potential spectrum assignments under a CBA-led auction. Under the CBA proposal and FCC rules, all prospective licensees must comply with the Commission's foreign ownership requirements under the Communications Act to receive FCC approval.

The CBA has provided unprecedented transparency about its proposal to date. On October 29, 2019, the CBA announced an agreement with rural and nationwide wireless carriers on key principles that should govern any bidding of C-band spectrum in a CBA-led auction. These principles include the following:

- Auction procedures will be made public before the auction and with FCC oversight.
- Reasonable bidder education efforts will be held consistent with prior spectrum auctions.
- Joint bidding agreements will be prohibited and ownership and agreement disclosures will be made public.
- The auction will be open to all qualified bidders consistent with FCC practice.
- The bidding process will be transparent, with: (i) no sealed bids; (ii) no combinatorial or package bidding; (iii) release of bid data round-by-round consistent with recent FCC auction information practice; and (iv) use of the FCC's limited information disclosure procedures to safeguard against anticompetitive conduct.
- All applicants must agree to be bound by the FCC's prohibited communication rules, including reporting obligations to, and enforcement by, the FCC.
- A portion of auction proceeds, in excess of those needed to cover the costs for the auction and the transition of the spectrum, will be returned to the U.S. Treasury.

These agreed-upon principles from industry stakeholders demonstrate broad support for an open private auction with procedural guardrails to ensure a fair and transparent outcome. Stakeholder alignment will pave the way for an expeditious sales process that is fair, transparent, well understood by potential buyers, and consistent with FCC process. By facilitating the expeditious clearing and assigning of C-band spectrum for the 5G services, the principles represent a huge win for all concerned—most importantly, for consumers, workers and businesses across the U.S.

If the FCC approves the CBA's proposal, CBA's member companies have committed to make a significant voluntary contribution to the U.S. Treasury. Moreover, as should now be clear, the CBA's members are undertaking considerable expense and risk, and the likely near term benefits to society from clearing this spectrum for terrestrial 5G use years faster than the alternatives will dwarf any future auction revenues. Simply put, concerns about "unjust enrichment", "windfall", and "speculation" are unfounded. Americans and the U.S. Treasury will benefit significantly from the proceeds of the CBA's proposal, which accelerates the innovations Americans will see from 5G deployment.

* * *

Thank you in advance for your consideration of our views. I ask that this letter be submitted into the record. Please contact me with any questions.

Respectfully submitted,

/s/ Peter Pitsch

Peter Pitsch
Executive Vice President, Advocacy & Government Relations
C-Band Alliance

Post-Hearing Questions for the Record
Submitted to The Honorable Christopher Krebs
From Senator Maggie Hassan

"Supply Chain Security, Global Competitiveness, and 5G"

October 31, 2019

Question#:	1
Topic:	5G Deployment
Hearing:	Supply Chain Security, Global Competitiveness, and 5G
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: In your testimony to the committee, you stated that "5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years, and coupled with the growth of cloud computing, automation, and the future of artificial intelligence, demands focused attention today to secure tomorrow." Significantly increased reliance on software over hardware in the 5G infrastructure increases the cybersecurity challenges through a greater attack surface. You also mentioned that a part of your effort to help shape the rollout of this emerging infrastructure is to work with other agencies, as well as industry, to increase security and resilience of 5G infrastructure at the design phase. What specific measures are you taking to assess and verify the secure-by-default design and deployment of 5G technologies?

Response: During these early stages of 5G, the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is focused on cross-collaboration and awareness until more mature use cases emerge in real world deployments. To that end, we are coordinating with the Department of Homeland Security's Science and Technology Directorate and are in close collaboration with the U.S. Department of Defense, as well as several of the National Laboratories, regarding research and development. DHS's research and development efforts are particularly focused on concepts related to Internet of Things and Open Radio Access Networks, which will test software vulnerabilities – this will create an enhanced understanding of use cases and future threats. We also work with industry partners to promote interoperability between vendors supporting 5G infrastructure and participate in international standards bodies, such as 3GPP and ITU. We are persistently engaged with our European partners through forums, such as the Prague 5G Security Conference.

CISA is also involved in the federal Chief Information Officer Council-Chartered Federal Mobility Group, which gathers over 200 experts from over 40 departments and agencies

Question#:	1
Topic:	5G Deployment
Hearing:	Supply Chain Security, Global Competitiveness, and 5G
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

to develop best practices, identify vulnerabilities, and produce guidance relating the 5G and mobile cyber security. CISA ensures the developments and lessons learned by this group are transferred to our private-sector partners, enabling a more resilient and secure national mobile infrastructure.

Question#:	2
Topic:	Risk Assessment
Hearing:	Supply Chain Security, Global Competitiveness, and 5G
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: The 5G technology offerings from suppliers based in the United States and in allied nations involves stitching together solutions from multiple software and hardware suppliers. While this approach creates a vibrant technology ecosystem, it introduces complexity and additional vulnerabilities with respect to interoperability, even among trusted suppliers. Given the complexity and scale, what are you doing to assess risk present in the end-to-end scenarios and to ensure that all the software and hardware solutions involved in critical infrastructure will fit together securely?

Response: At CISA, we have conducted a broad review of the risks posed by 5G technology and have posted a risk product (e.g., 5G Risk Characterization Paper) on our website. CISA also supports risk assessments for the Committee on Foreign Investment in the United States, Team Telecom, and the Federal Acquisition Security Council. CISA engages with the Information Technology and Communications sectors to better understand the opportunities and challenges these key stakeholders, especially for 5G deployment, will face in security and resilience.

Question#:	3
Topic:	Trusted Supplier
Hearing:	Supply Chain Security, Global Competitiveness, and 5G
Primary:	The Honorable Margaret Wood Hassan
Committee:	HOMELAND SECURITY (SENATE)

Question: 5G infrastructure buildout presents substantial supply chain security risks. The entire life-cycle of development, deployment, operation, and maintenance of network infrastructure, services, and devices will introduce potential sources of vulnerability and opportunities for malicious activity. What is your definition of a trusted supplier, how did you develop this definition, and what are you doing to assess risks associated with all stages of the development life-cycle in the 5G ecosystem?

Response: CISA has developed criteria that can be used to evaluate a company for further investigation by following the principles that focus on: 1) The functionality and other vulnerabilities of the product or service, 2) The countries in which the supplier and its component suppliers have operations, including risks arising from the legal regimes of those countries, and 3) The personal, professional, and other ties between the supplier and its leadership and foreign governments.

Question for the Record submitted to
Deputy Assistant Secretary Robert L. Strayer by
Senator Maggie Hassan
October 31, 2019
U.S. Senate Committee on Homeland Security & Governmental Affairs

Question:

In your testimony to the committee, you stated that the United States is leading on the development of 5G technical standards in the international standards setting forums. Specifically, you stated that the United States is well represented at the World Radio Conference, citing a delegation of "120 people from the private sector and the government attending this international conference on worldwide spectrum policy."

How will you assess the delegation's success engaging with the 193 nations at this conference and effectiveness in moving our spectrum policy forward?

Answer:

The 2019 World Radiocommunication Conference (WRC-19) will address approximately 36 agenda items, ranging from consideration of additional global spectrum allocations for mobile broadband services to improvements for Earth Stations in Motion (ESIMs) and High-Altitude Platform Systems (HAPS). We will assess the delegation's success at WRC-19 by our ability to advance U.S. interests, such as the use of innovative new services and systems, more efficient uses of spectrum, and coordination of mega-constellation satellite systems, while also taking into account critical commercial and government systems and providing appropriate protections for incumbent services, as needed.

Committee on Homeland Security and Governmental Affairs
United States Senate

Post-Hearing Questions for the Record
Submitted to The Honorable Jessica Rosenworcel
From Senator Maggie Hassan

"Supply Chain Security, Global Competitiveness, and 5G"

October 31, 2019

The Honorable Jessica Rosenworcel, Commissioner, Federal Communications Commission

1. **Would you please elaborate on the ways that the FCC can facilitate the development of an open radio access network (RAN)? Specifically, what resources would the FCC need to develop testbeds for open RAN development in the United States?**

We need an approach to supply chain security that recognizes that despite our best efforts, secure networks in the United States will only get us so far because no network stands by itself. Our networks still will connect to insecure equipment abroad. So we need to start researching how we can build networks that can withstand connection to equipment vulnerabilities around the world.

One way to do this is to invest in virtualizing radio access networks—or open RAN. The RAN is the most expensive and restrictive part of the network. Today, all major components of a RAN have to come from the same vendor. There is no way to mix and match. But if we can unlock the RAN and diversify the equipment in this part of our networks, we can increase security and push the market for equipment to where the United States is strongest—in software and semiconductors. This also will give carriers around the world that are locked into upgrade cycles with a single foreign vendor a way out.

The FCC can help with this effort. First, the FCC should coordinate with other agencies to ensure no single vendor dominates networks. The FCC also should work with the Department of State and the Department of Commerce in particular to extend this approach abroad, too. Second, the FCC can encourage the development of the testbeds in the United States that bring together operators, vendors, vertical interests, and other government agencies to support these models. We can start that effort right now simply by making it a priority. Earlier this year, the FCC announced the creation of two Innovation Zones in New York City and Salt Lake City. These Innovation Zones are city-scale test beds for advanced wireless communications and network research, including 5G networks. In New York City, the Innovation Zone will support Cloud Enhanced Open Software Defined Mobile Wireless Testbed for City-Scale Deployment, or COSMOS. In Salt Lake City, the Innovation Zone will support a Platform for Open Wireless Data-driven Experimental Research with Massive MIMO Capabilities, or POWDER.

Innovation zone partner universities and the cities themselves will enable test bed development and deployment, supported by the National Science Foundation along with a consortium of telecom and technology companies. However, the FCC could encourage or require that the network deployed to support this research be compatible with open RAN architectures. Then we could do the same as we authorize additional Innovation Zones throughout the country.

2. **The FCC would need to coordinate with other government agencies to develop an Open RAN. Would you please describe the interactions the FCC has had with the relevant agencies on those efforts, and what the next steps would be to facilitate that coordination?**

Last month, the bipartisan leadership of the United States Senate Committees on Homeland Security and Government Affairs, Intelligence, Foreign Affairs, and Armed Services wrote the White House expressing concern that we do not have a coordinated, national strategy in place for 5G—and we need one. I agree.

Last year the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology and Supply Chain Risk Management Task Force. This public-private partnership will develop recommendations to identify and manage risk in the global supply chain. The Task Force includes representatives from the Department of Homeland Security as well as experts from the Department of Defense, Department of Treasury, General Services Administration, Department of Justice, Department of Commerce, Office of the Director of National Intelligence, and the Social Security Administration. In addition, there is expertise from industry, with representatives from communications carriers, equipment manufacturers, and cybersecurity companies.

It's an impressive list—but the FCC does not have a seat at the table. It was left off the executive committee of the Task Force. Leaving the agency with primary oversight over communications out is neither prudent nor wise—especially because we have ongoing proceedings that speak directly to the issues covered by the Task Force.

The FCC should be added to the executive committee of the Task Force. We should be working together to develop a common approach to 5G security.

3. **Both licensed and unlicensed spectrum will be critical to unlocking the full potential of 5G and the Internet of Things for the public. The FCC has begun proceedings on unlicensed spectrum in the 6 GHz band, and on shared commercial use in the 3.5 GHz band. However, as you noted in your remarks, additional mid-band spectrum is necessary for a functional 5G system, especially for rural deployment of 5G technology. There are multiple competing proposals in front of the FCC right now concerning what to do on the 3.7 – 4.2 GHz band ("C-Band"). I would urge you and your fellow commissioners to carefully consider the proposals in front of you, and evaluate them on how they protect taxpayer dollars and respect that spectrum is a public resource. How will the FCC ensure that the mid-band spectrum that the U.S. allocates for 5G usage is**

a standard-driver globally in the face of differing European and Chinese spectrum allocation?

It is important that we do not limit our discussion about security to network equipment. We need to go beyond discussing these problems and get to what is fundamental—and that is spectrum. By bringing the right airwaves to market, we can help broaden the market for secure equipment.

On that front, the FCC has work to do. Its early efforts to support 5G wireless service have focused on bringing only high-band spectrum—known as millimeter wave—to market. These airwaves have significant capacity, but also real propagation challenges. As a result, commercializing them is costly—especially in rural areas. This means our early 5G spectrum policy could create 5G haves and have-nots, deepening the digital divide that already plagues too many rural communities nationwide.

This sets us apart from most countries in the world, which are looking to mid-band spectrum for their early 5G wireless deployments. While this spectrum has less capacity than millimeter wave, its signals travel further. That means deployment is more feasible in more places because fewer terrestrial facilities are required to make it work.

Our failure to act early on mid-band spectrum has security consequences. In many of these bands, there is only one Chinese vendor offering equipment. That means countries building their 5G networks using these airwaves do not have a competitive choice for secure equipment.

In the United States we have unique skill and scale. That means where deployment takes place here, vendors follow. So it is time for the FCC to make it a priority to make mid-band spectrum available, too. If we can do that, our carriers will build there and more vendors will compete to offer service. And when we expand the market for secure equipment at home, it also grows abroad.

To this end, I have advocated for expediting the 3.5 GHz band auction. Comparable airwaves are being deployed abroad for new 5G service and I believe the United States should act fast to ensure its global leadership in this band. It is also necessary to identify a path forward to expand opportunities for terrestrial use for 5G service in the 3.7 – 4.2 GHz band, as you suggest.

Committee on Homeland Security and Governmental Affairs
United States Senate

Post-hearing Questions for the Record
Submitted to Hon. Jessica Rosenworcel
From Senator Kyrsten Sinema

"Supply Chain Security, Global Competitiveness, and 5G"

The Honorable Jessica Rosenworcel, Commissioner, Federal Communications Commission

1. **The FCC has a long history of bringing telehealth services to patients in rural areas. Telehealth has been particularly beneficial to veterans in rural areas, specifically those suffering from posttraumatic stress disorder who can be uncomfortable travelling long travel distances.**

   In Arizona, providers are utilizing telehealth to provide veterans' health care that is accessible, flexible, and patient-centered. However, veterans in underserved or unserved parts of the state face significant challenges to access telehealth services. While I am pleased to see the opportunities that telehealth services provide for veterans, I am concerned that not all patients in Arizona can use these services because of lack of access to wireless at home.

   What is the FCC doing to support innovation in telehealth and also ensure that veterans in rural areas with limited access to broadband are not left behind in the race to 5G?

   The healthcare industry is challenged by both high costs and limited access, and advances in 5G can help address both these issues. But this will only happen if the benefits of 5G are made available to all Americans—including Americans in our most rural areas, where the business case for deploying 5G is hardest.

   The FCC has long had a Rural Health Care program, which is comprised of two sub-programs – the Telecommunications Program and the Health Care Connect Fund. In combination, these sub-programs provide funding to eligible health care providers for telecommunications and broadband services necessary for the provision of health care. In addition, earlier this year, the FCC kicked off a rulemaking on a new Connected Care Pilot Program. Through this connected care effort, the agency would be seeking to better understand the nexus between patient connectivity to their health care provider and health outcomes. The agency's proposal is specifically targeted at low-income Americans and veterans. As this effort moves forward in the next year, I am hopeful that it will generate meaningful data to inform policymakers in the future.

Finally, the RAY BAUM's Act of 2018 required the FCC to "submit to Congress a report on promoting broadband Internet access service for veterans, in particular low-income veterans and veterans residing in rural areas." Our report found that many veterans still lack access to fixed broadband, mobile broadband, or both. Barriers to access include lack of deployment where they live, price, and in some cases, digital illiteracy. Ensuring all veterans enjoy the benefits of broadband access is critical, especially because this may be a population especially primed to benefit from new connected care initiatives.

2. **The May 2019 FCC Report on Broadband Deployment in Indian Country noted approximately 47 percent of houses on rural Tribal lands have access to broadband. As you know, Educational Broadband Services (EBS) resides in the mid-band spectrum, in the 2.5GHz band and has help foster programs that tackle the homework gap and digital divide by providing spectrum for broadband services. In Arizona, the Havasupai Tribe uses EBS channels for wireless routers for their members to take online classes. The Tribe was recently granted four new EBS channels that they indent to use for telemedicine.**

   In 2018, the FCC began a process to consider updating the framework for licensing EBS spectrum in the 2.5 GHz band. The proposed rule included priority filing windows for Tribes to apply for EBS licenses before issuing licenses for any remaining spectrum through auction.

   First, I want to thank the Commission for establishing a Tribal Priority window for new EBS license issuance for Tribal National in the final rule. This decision provides Tribes with the opportunity to expand rural broadband, accelerate 5G deployment, close the digital divide, and bridge the homework gap.

   It is critical that we work with tribal entities to determine the length of the priority filing window. That is why I sent a letter to Chairman Pai urging the FCC to open the priority filing window for Tribes for 180 days for education and application purposes.
   It is my understanding based on information from Tribes in Arizona that 180 days is sufficient to ensure Tribes have the opportunity to learn about the logistics of application to EBS spectrum prior to the opening of the priority filing window.

   Has the Commission determined when the filing window will open and for how long it will be open for?

   The Rural Tribal Priority Window will open on February 3, 2020, and it will be open for 180 days.

   If not, how will the agency work with tribal entities to ensure the window time is sufficient?

The FCC has determined when the filing window will open and for how long it will be open. But we still have a long way to go to honor our federal trust responsibility to Tribal communities that have been impacted by the FCC's decisions. That's why, last year, I called on the FCC to update the Commission Statement of Policy on establishing government-to-government relationship between the agency and federally-recognized Tribes. This document has not been revisited since it was adopted more than a decade and a half ago. It is time to take on this task and do it in conjunction with resolving longstanding issues around infrastructure deployment. In doing so, we can set a clear and updated course for FCC policy while also giving substance to Tribal self-determination.

3. **According to a report from the Defense Innovation Board, 5G has the ability to enhance Department of Defense decision-making and strategic capabilities from the enterprise network to the tactical edge of the battlefield. Has the FCC been engaged with the DOD regarding DOD current and future needs related to 5G technology?**

In the first instance, those engagements happen through the Chairman's Office or through staff-to-staff discussions on specific spectrum bands that require coordination. But, as the Defense Innovation Board recognized, 5G ecosystems of technology can both "revolutionize DoD operations" and also "present[] a serious potential risk for DoD going forward." That means more meaningful engagement between the FCC and the DoD is critical. At a minimum, close coordination with both DoD and the National Telecommunications and Information Administration will be important to clear and reassign spectrum below 6 GHz that will be important to both commercial and government 5G use cases.

4. **How does the FCC coordinate with the National Telecommunications and Information Administration (NTIA) and the DOD on spectrum allocation and management for changing DOD priorities? In particular, what roles do the FCC and NTIA perform related to DOD actions to share, clear, or request different spectrum? How long do these actions typically take?**

Growing demands on our airwaves suggest we need new and more efficient ways of addressing spectrum allocation. Federal authorities have substantial spectrum assignments. After all, critical missions throughout the government are dependent on access to our airwaves.

Our traditional processes for repurposing federal spectrum essentially involve three steps: clear, relocate, and auction. But this three-part command that has worked well in the past may work less well going forward. Just as in the commercial sector, more government functions than ever before are traveling over our airwaves and it is growing harder to find spectrum for federal relocation.

More recently, we have explored sharing of federal and commercial spectrum resources. This is an exercise in innovative thinking, and its success depends on the development of new dynamic databases and bi-directional sharing.

These efforts are still worth pursuing. But we also need new approaches—one that will facilitate federal repurposing better than our old three-step process. We should consider developing a series of incentives to serve as the catalyst for us to identify more spectrum for relocation. For example, what if we were to financially reward federal authorities for efficient use of their spectrum resources? What if they were able to reclaim a portion of the revenue from the subsequent reauction of their airwaves? Would they make new choices about their missions and the resources they need to accomplish them? I believe this is an idea worth exploring.

5. **Does the federal government have a Federally Funded Research and Development Center or a University Affiliated Research Center related to FCC, NTIA, and DOD coordination regarding 5G and 5G technology? If not, could such a center be beneficial?**

Various federal efforts are facilitating research and development of 5G and 5G technology. For example, the National Science Foundation's Platforms for Advanced Wireless Research has been cited as an example of how the U.S. is leading the way in wireless technology innovation. The program's initial testbed sites have been named as the FCC's first-ever Innovation Zones for spectrum research and development. In addition, the Department of Defense's National Spectrum Consortium is funding research into 5G and 5G-based technology, and is compromised of leading technologists, engineers, scientists, manufacturers, and program managers from industry, academia, and government. The Networking and Information Technology Research and Development Program's Wireless Spectrum Research and Development Interagency Working Group coordinates federal spectrum-related research and development activities. Finally, the National Institute of Standards and Technology also is funding early research related to 5G and advanced wireless communications.