RPTR MERTENS

EDTR ROSEN

LEGISLATING TO SECURE AMERICA'S WIRELESS FUTURE

FRIDAY, SEPTEMBER 27, 2019

House of Representatives,

Subcommittee on Communications

and Technology,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to notice, at 9:28 a.m., in Room 2123, Rayburn House Office Building, Hon. Mike Doyle [chairman of the subcommittee] presiding.

Present: Representatives Doyle, McNerney, Clarke, Veasey, Soto, O'Halleran, Eshoo, Butterfield, Matsui, Schrader, Cardenas, Pallone (ex officio), Latta, Shimkus, Kinzinger, Bilirakis, Johnson, Long, Flores, Walberg, Gianforte, and Walden (ex officio).

Staff Present: AJ Brown, Counsel; Jeff Carroll, Staff Director; Parul Desai, FCC Detailee; Evan Gilbert, Deputy Press Secretary; Waverly Gordon, Deputy Chief Counsel;

Tiffany Guarascio, Deputy Staff Director; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Jerry Leverich, Senior Counsel; Dan Miller, Senior Policy Analyst; Meghan Mullon, Staff Assistant; Phil Murphy, Policy Coordinator; Tim Robinson, Chief Counsel; Andrew Souvall, Director of Communications, Outreach and Member Services; Rebecca Tomilchik, Staff Assistant; Mike Bloomquist, Minority Staff Director; Michael Engel, Minority Detailee, Communications & Technology; Margaret Tucker Fogarty, Minority Legislative Clerk/Press Assistant; Peter Kielty, Minority General Counsel; Bijan Koohmaraie, Minority Deputy Chief Counsel, CPAC; Zack Roday, Minority Communications Director; and Evan Viau, Minority Professional Staff Member, Communications & Technology.

Mr. Doyle. The Subcommittee on Communications and Technology will now come to order. The chair recognizes himself for 5 minutes for an opening statement.

Good morning, and welcome to the Subcommittee on Communications and Technology's legislative hearing on Legislating to Secure America's Wireless Future. Today, the subcommittee will consider a number of legislative proposals that address challenges from spectrum management to securing our Nation's telecommunications infrastructure. The proposals before the subcommittee today are H.R. 4462, the Studying How to Harness Airway Resources Efficiency Act, or the SHARE Act, which I have introduced with my good friend, Ranking Member Latta. This legislation would require NTIA to establish a spectrum-sharing strategy for Federal entities using advanced technologies, such as artificial intelligence, automated frequency coordination, and environmental sensing to facilitate more efficient spectrum sharing and use by the Federal Government. The bill would also require the FCC to report to Congress on the feasibility of using existing sharing technologies on several important spectrum bands.

As we look towards the future, it is necessary for every licensee to use spectrum more efficiently, the Federal Government being chief among them. We need to find ways to modernize how the government uses and shares spectrum amongst agencies and departments, as well as with the commercial sector.

The CBRS band is a great example of how sharing can effectively accommodate a wide range of users and a wide range of uses. Just yesterday, the FCC voted on an order to sell licenses in the CBRS band, and a few weeks ago, the band officially launched for commercial operations. This band will combine licensed, unlicensed, and Federal incumbent users in one band while protecting incumbents' rights and ensuring that the

spectrum is always available for use. My hope is that the SHARE Act can act as a bridge to future innovative sharing videos like we see in the CBRS band.

Next, we have H.R. 4461, the Network Security Information Sharing Act, introduced by myself and my colleague, Congressman Kinzinger. This legislation would establish an information-sharing program at the Department of Homeland Security to share the supply chain security risk information with the telecom industry. This legislation would help all providers, but most importantly, small and rural providers that lack the resources and expertise to engage here in Washington, with what has largely been closed-door discussions related to the threats of untrusted equipment vendors. Our hope is that by creating a program with an inclusive mandate that these providers will be more able in the future to avoid deploying in technologies that pose an outside risk to their customers and to the nation.

After that, we have H.R. 4459, the Secure and Trusted Communications Network Act, introduced by Chairman Pallone and Ranking Member Walden, which would require the FCC to create a list of equipment and services that pose unacceptable risk to national security. It would authorize a fund to unable telecommunications carrier with unsafe equipment in their networks to remove it and replace it with trusted equipment and services. Telecom service is far too essential for any of our Nation's carriers to be using untrusted elements in their network.

The subcommittee will also consider H.R. 2881, the Secure 5G and Beyond Act, introduced by Representatives Spanberger, O'Halleran, Brooks, Rooney, and Slotkin. It would require the government to work with strategic allies to secure their 5G networks, and ensure that U.S. 5G networks are secure and work with industry to guard against foreign political influence.

Next, we will consider the Promoting United States Wireless Leadership Act of 2019 introduced by Representatives Walberg and Dingell. We will also consider H.R. 2063, the E-FRONTIER Act, introduced by Representatives Cardenas and Brooks. And finally, we will discuss House Resolution 575, expressing the sense of the House that all stakeholders in the deployment of 5G should consider and adhere to the Prague proposals, which was introduced by Representatives Flores and Soto.

I also want to thank all the witnesses for being here today. I want to recognize Ms. Stempfley for participating. She is currently Director of the CERT Division at the Software Engineering Institute at Carnegie Mellon University in Pittsburgh, which is the heart of my congressional district. We are always glad to have someone from CMU up here on the panel. Previously, she served as Acting Assistant Secretary in the Office of Cybersecurity and Communications at the Department of Homeland Security, and she established and led the Department of Defense's computer emergency response team. So I want to especially thank her for appearing before the subcommittee today.

So I look forward to a discussion of all of these proposals, and now, the chair recognizes Mr. Latta, ranking member of the subcommittee, for 5 minutes for his opening statement.

Mr. Latta. Well, thank you very much, Mr. Chairman, and thank you very much for calling today's hearing, and I also want to thank our witnesses for being with us today as we discuss legislation on our network supply chain security and management of our spectrum resources.

There are several bipartisan bills on today's hearing that address the challenges we face to ensure our critical communications infrastructure is secure from vulnerabilities. I am especially pleased to have worked with our subcommittee chairman,

the gentleman from Pennsylvania, on H.R. 4462, the SHARE Act, to empower our agencies to facilitate innovative spectrum sharing strategies to more efficiently use our airwaves.

As the executive branch agency principally responsible for advising the President on spectrum and telecommunication matters, NTIA should continue to play the lead role directing a collective government approach to managing the Federal Government's access to spectrum resources. This bill helps empower NTIA to use tools to meet the challenge of growing wireless needs into the 21st century.

Today's hearing also features several bills to addresses vulnerabilities in our Nation's communication networks, such as the inclusion of unsecure equipment. Many providers' networks contain equipment supplied by suspect foreign carriers. However, this is only because the provider didn't understand the associated risks. The bill before us seeks to prevent this type of situation from occurring on a forward-looking basis. Understandably, these providers are in a period of uncertainty, and although they may want to do their part to protect national security, they may need help doing so.

The FCC has voiced concerns about the network security and proposed prohibiting USF recipients from using controversial equipment. So as winners of the FCC's latest Connect America Fund II reverse auction comes to grip with the buildout requirements accompanying these funds, it is critical that we work in a bipartisan way to ensure that they can revisit how those conditions impact the winning bid in order to keep their equipment free from security vulnerabilities.

Not only do we want to prevent the Federal funding to pay for gear that may pose a national security risk, but we do not want winners of CAF auctions to be put in an unattainable position of not being able to meet buildout requirements now that their cost estimates may have changed.

I want to thank, again, to our witnesses for being with us today and for the testimony today, and I am going to yield the rest of my time to the gentleman from Illinois.

Mr. Kinzinger. Well, thank you, Mr. Chairman, for yielding. The security of American communications and information networks is paramount to national security. It is a field I know fairly well from my time in the military. But the sword cuts both ways. As we have seen through the years, certain foreign adversaries have systematically coerced their equipment manufacturers to embed back doors and other capabilities into their products which are later purchased by American companies and integrated into our networks. No foreign actor should have the ability to eavesdrop on U.S. citizens or our government, and let alone use these back doors to launch cyber attacks or disrupt our communications.

In an effort to help the private sector avoid purchasing or installing this dangerous equipment, I have worked with the chairman, Chairman Doyle, to introduce H.R. 4461, the Network Security Information Sharing Act, which will be part of the discussion here today. So I look forward to that discussion, and I yield back to my friend.

Mr. Latta. Mr. Chairman, I yield back the balance of my time.

Mr. Doyle. The gentleman yields back.

The chair now recognizes Mr. Pallone, chairman of the full committee, for 5 minutes for his opening statement.

The Chairman. Thank you, Chairman Doyle. Today, we are considering a series of bills to secure America's wireless future that will ensure that the government manages Federal and commercial spectrum more efficiently to promote innovation and better serve all Americans. It will also guarantee that our wireless networks are secure from

foreign adversaries that may wish to spy on Americans or do us harm.

I applaud the work of Chairman Doyle and Ranking Member Latta introducing the SHARE Act. Their bill will cement the longstanding policy that our Nation's key agencies, the National Telecommunications and Information Administration, and the Federal Communications Commission, remain responsible for spectrum policy. These expert agencies can act as impartial judges to balance the demands and interest of spectrum stakeholders such as the Department of Defense, the Federal Aviation Administration, public safety and commercial carriers.

At our hearing in July, we heard that the management of Federal Government spectrum requires a strong central voice at NTIA, and I think the SHARE Act does a great deal to help NTIA meet the mission critical needs of government agencies in a more efficient and modern way. The FCC, likewise, must remain in the driver's seat when it comes to commercial spectrum. And for that reason, I am pleased the SHARE Act requires the FCC to look for ways to expand and improve the revolutionary spectrum sharing techniques being rolled out in the citizens broadband radio service.

When it comes to securing these networks from foreign adversaries, I want to thank Ranking Member Walden and Representatives Matsui and Guthrie for partnering with me to introduce the Secure and Trusted Communications Networks Act. Our legislation will prohibit the spending of Federal dollars on suspect communications equipment and services that undermine national security. Our bill also establishes a $1 billion reimbursement program to help small carriers remove compromised equipment and replace it with secure alternatives.

As we have heard, much of the global supply chain for telecommunications equipment flows through China at one point or another. And Chinese industrial policies

allow state-run manufacturers like Huawei to sell suspect equipment to American providers cheaper than nearly everyone else. Although many of the bigger carriers have avoided these threats, it still is a significant issue for smaller and more rural carriers who built their network using suspect equipment.

Communications networks are interconnected, and that means that one weak link can harm the whole system. We must help smaller carriers remove suspect equipment for the good of the entire country. Representatives Kinzinger and Chairman Doyle also have legislation on this point that would help the Federal Government better share supply chain risk information with the communications providers.

So I look forward to hearing from our witnesses, and I also wanted to briefly recognize or mention that Dean Brenner on today's panel, who is a fellow Monmouth, New Jersey, native. Glad to see you here today. Welcome.

And with that, I yield the balance of my time to Ms. Matsui.

Ms. Matsui. Thank you very much. I am pleased that we are considering H.R. 4459, the Secure and Trusted Communications Networks. This bill will create a new fund that provides financial incentives to small and rural wireless providers to replace certain equipment of Huawei and ZTE with new equipment that includes secure hardware and software capabilities.

Mr. Chairman, we must continue to consider policies as per U.S. leadership and innovation in the 5G race. H.R. 4459 will help provide additional security for America's telecommunications providers. Still, more needs to be done with regard to America's spectrum policy. That includes smart spectrum policies for both licensed and unlicensed use for 5G and beyond. We must explore opportunities to option the C-band. My bill, the WIN 5G Act, strikes the right balance by aiming to clear at least 300 megahertz of

spectrum, and is supported by a broad range of stakeholders, including public interest groups and industry stakeholders. I continue to work with Chairman Doyle on this issue.

Additionally, Congressman Guthrie and I introduced the SPECTRUM NOW Act, that can provide a pathway to make an additional 100 megahertz of spectrum available. A balanced approach to the introduction of wireless services is not only critical, but necessary for expanding the use in the 6 gigahertz band. I also continue to focus on resolving a 20-year-old debate over the 5.9 gigahertz band. I'm hopeful that the FCC will consider new rulemaking to address this band soon.

And with that, I yield back to the chairman.

Mr. Doyle. The chairman yields back. The gentleman yields back.

It is now my pleasure to recognize who just made his grand entrance, my good friend, Mr. Walden, ranking member of the full committee for 5 minutes.

Mr. Walden. Thank you, Mr. Chairman. On time, on budget right here.

I want to welcome our witnesses. Thank you for being here. Your insight will be another important input to the process we began last Congress on how best to secure our communications networks. Our Nation's telecommunications infrastructure represents the lifeblood of preserving a free and open society, as we all know, and any effort to disrupt that infrastructure should be taken as an effort to undermine our liberties.

The bills before us today deliver on a commitment we began last Congress, and that commitment is to have a bipartisan process to mitigate these threats and to secure this sector going forward. Moreover, I know Chairman Pallone and I agree that the Energy and Commerce Committee is singularly able to speak to these topics in the Congress. And with both sides working together with stakeholders ranging from industry to civil society, we can do so successfully.

Everyone in this room can agree on the importance of securing our Nation's communications networks from vulnerable equipment. In fact, we heard testimony over 2 years ago on the vulnerabilities that exist in these networks. We also heard of the impact on rural providers who may be more disproportionately impacted by calls to replace existing equipment as they seek to stay in their budgets, not to mention within Federal programs purchasing guidance to deploy the most effective products.

Unfortunately, our adversaries have no reservations about one way or another subsidizing their pet companies, and thus, they become attractive options for the budget-sensitive providers. I have seen how small broadband providers in my own state are trying to make a go of deploying broadband networks and stretching limited funds to ensure they connect with the most constituents in some of the hardest to reach places, and you can certainly find those in my district. Many of these providers don't have an army of consultants with the necessary security clearances to fully appreciate the vulnerabilities that do exist and how to inform their purchasing decisions.

For those who receive Federal support to build out broadband networks in unserved areas, like many of the providers in my district, we cannot set them up for failure by requiring them to select the lowest cost equipment option, only then for Uncle Sam to later say Oh, by the way, well, not that lowest cost equipment, so we need to get this right.

H.R. 4461, the Network Security Information Sharing Act, would facilitate exactly the type of information sharing needed by rural providers that have vulnerable equipment in their networks. This was the centerpiece of our bipartisan discussions in the last Congress, and I am pleased to see this concept taking shape in today's hearing.

H.R. 4459, the Secure and Trusted Communications Networks Act, which I am an

original co-sponsor of, would further address this problem by setting up a reimbursement program to rip and replace vulnerable equipment from these networks. But we still have some details to work on out the way to markup the program is modeled on the FCC so far successful broadcast incentive repack reimbursement program. We need to get this right. It is critical to our national security, but also to our competitiveness as we start rolling out new technologies.

This brings me to another topic that I raised in our July spectrum hearing of how Russia is seeking to influence our public discourse on the subject of deployment of next generation networks. I know Congresswoman Eshoo and Congresswoman DeGette also shared my concern at that hearing. As we continue our work to close the digital divide and lead the race to 5G, we must be prepared to prevent threats from those seeking to diminish America's standing in the world.

Just this past week, my staff saw this card which was posted on a bulletin board by the Rayburn cafeteria. Now, the details are pretty scant, who is behind this campaign, and just lists a litany of issues why 5G is supposedly bad.

It collects numerous stories around the country on things wrong with 5G. Ironically, one of those stories about a community health fears stopping a 5G rollout in Australia, while at the same time, noting that the World Health Organization stated there should not be any health risk from 5G. And the Cornell University research showed 5G networks to be safer than previous networks.

So we have to be vigilant. We have to be vigilant about efforts to influence our thinking in this space, and I hope the committee will look ahead at other efforts being pursued to stifle our internet architecture.

I look forward to hearing about the other bills put forward by our members today,

Mr. Chairman, as thoughtful approaches to these challenges. So thanks again for having this hearing, and I do hope the full committee or the oversight committee, or this committee, will do some looking into what is being pushed out there in the public side and who is behind it. So we need the facts.

Thank you, and I yield back.

Mr. Doyle. I thank the gentleman. The gentleman yields back. The chair would like to remind members that pursuant to committee rules, all members' written opening statements shall be made part of the record.

So I would like to introduce our witnesses for today's hearing. Ms. Bobbie Stempfley, Managing Director, CERT
Division, Software Engineering Institute at Carnegie Mellon. Thank you for being here today. Mr. John Nettles, the president of Pine Belt Wireless. Mr. Nettles, thank you for being here. Mr. Harold Feld, Senior Vice President, Public Knowledge. Harold, thank you again. And Mr. Dean Brenner, Senior Vice President, Spectrum Strategy and Tech Policy for Qualcomm, Incorporated. Mr. Brenner, thank you. We want to thank all of you for joining us today. We look forward to your testimony.

At this time, the chair will now recognize each witness for 5 minutes to provide their opening statement. Before we begin, I would like to explain the lighting system. In front of you is a series of lights. The light will initially be green at the start of your opening statement. It will turn yellow when you have 1 minute remaining. Please begin to wrap up your remarks at that point, and when the light turns red, we are just going to cut your microphones off.

So Ms. Stempfley, you are now recognized for 5 minutes.

STATEMENTS OF BOBBIE STEMPFLEY, MANAGING DIRECTOR, CERT DIVISION, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY; JOHN NETTLES, PRESIDENT, PINE BELT WIRELESS; HAROLD FELD, SENIOR VICE PRESIDENT, PUBLIC KNOWLEDGE; AND DEAN R. BRENNER, SENIOR VICE PRESIDENT, SPECTRUM STRATEGY & TECH POLICY, QUALCOMM INCORPORATED

STATEMENT OF BOBBIE STEMPFLEY

Ms. Stempfley. Thank you.

Mr. Doyle. Hit your microphone button there.

Ms. Stempfley. There we go. One additional light. Thank you very much.

Good morning. Chairman Doyle, Ranking Member Latta, members of the committee, thank you very much for the opportunity to participate in this hearing today and speak on supply chain risks in the telecommunications industry.

As has been said, I have been a public servant working in information technology focused on the application of information and technology to national security and public safety missions for more than 25 years. I am currently serving as the managing director at the CERT Division at Carnegie Mellon University Software Engineering Institute, where we focus on partnering with government industry, non-government organizations, and academia doing applied research to improve security and resilience of computer systems, information, and networks.

The telecommunications sector is a global system made of companies, suppliers, and users, that make communications possible. Because the telecom industry is

responsible for the flow of information, it is inextricably linked to how we work, play, and live, and plays a central role in the fundamental operations of society from business to government to families. The explosion of devices, new methods of computing, IoT devices within the infrastructure has only increased the attack surface, and, therefore, the responsibility of telecoms to participate in the overall protection and defense efforts.

Ultimately, the supply chain for the telecommunications industry is vital to achieving security at scale. Historically, checks and balances in the supply chain have been largely procedural such as licenses, warranties, regulations, legal resource, supplier reputation and have reasonably assured against defects and service failures.

Unfortunately, these controls are increasingly inadequate when applied to global supply chains for the complex information and communications technology and technology-based services that underpin critical capabilities in this industry.

An ever-expanding supply chain means that external dependencies must be rigorously measured and strategically managed for an organization to remain resilient. This includes addressing key areas in manufacturing and integration of the supply chains, in service supply chains, and in software supply chains. The ramifications of an attack anywhere on the telecommunications infrastructure could spread well beyond the point of origin and have the potential to affect entire nations, businesses, and private citizens. We must address not only the hardware, but the software and services as well.

The bills today, including the Secure and Trusted Communications Network Act of 2019, and the Network Security Information Sharing Act of 2019 are a very good first step in this security.

As the appropriate entities begin to implement supply chain security, encouraging resilience as a criterion at every stage of development and supply of information and

communications technology must continue to be the forward-leaning focus of the software and supply chain assurance efforts within government and industry.

Attacks against our supply chains unite acquirers and suppliers in search of scalable means for securing information about ICT risks that arise through malice or negligence. Suppliers and acquirers need standardized methods for conveying information about common issues related to both the hardware and software aspects of ICT, especially regarding non-conforming products that contain counterfeit, tainted, or defective components and can cause subsequent harm.

Fundamentally, the outcomes and risks factors we are seeking to manage are simple, even though the methods to accomplish them are not. First, suppliers must follow practices that reduce supply chain risks; second, products provided by suppliers are acceptably secure; third, the methods of distribution and/or transmission of the product to the purchaser guard against tampering; and finally, the product or service is used and sustained with acceptable security.

The acquisition security framework and the external dependencies management element of CERT's cyber resilience management model, which was developed and validated through research done by CERT researchers demonstrates that the following practice areas are elements of a mature supply chain risk management effort: Establishment and management of key relationships, engineering practices, secure product operations of sustainment, and an understanding and management of supply chain technologies, and overall infrastructure.

As private and public functions grow ever more inseparable from the information technology systems that support them, healthy public/private partnerships become even more necessary. To protect this infrastructure against growing and evolving cyber threats

requires a layered approach. The government's role in this effort is to share information and encourage enhanced security and resilience while identifying and addressing gaps not filled by the marketplace.

Information pertinent to the supply chain such as vulnerabilities, attack factors, supplier security information should be shared along with mitigation plans to those who need it. Actionable and usable information sharing must recognize the differing capabilities and roles of all participants and are key to successful sharing programs. Lastly, we must guard against the false choice between security and innovation. Thank you.

[The prepared statement of Ms. Stempfley follows:]

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

Mr. Doyle. Thank you very much.

Mr. Nettles, you are now recognized for 5 minutes.

STATEMENT OF JOHN NETTLES

Mr. Nettles. Chairman Doyle, Ranking Member Latta, members of the subcommittee, thank you for the opportunity to testify about securing communications networks and the support needed to keep rural America connected.

Pine Belt is a family-owned-and-operated company established by my father in the late 1950s. Over the years since, we have worked hard to keep pace with technology and to keep the company in the family. We launched our wireless network in 1995, with three analog sites covering two counties. We have grown that to 65 sites, and now provide 4G LTE across five counties, including many areas where ours is the only signal present. Not only do our customers depend on our network, but in an average day, we provide service, wireless voice and data connectivity, to as many as 30,000 visitors, most of whom are just passing through.

Pine Belt fully supports efforts to harden today's telecom networks for robust cybersecurity and to protect against potential national security threats. Yet, while the industry buzzes with excitement of the great things that will come from 5G network buildout, we and many other small companies across the country have been virtually frozen since early last year by the security concerns of our currently deployed equipment.

Pine Belt's modern network was rebuilt just a few years ago with equipment from ZTE through our participation in the Mobility Fund Phase I process, a reverse auction in

which winning bidders were those showing the lowest cost to serve the greatest number of road miles. Our main performance criterion was to provide as much coverage as possible as inexpensively as possible. We solicited quotes from five different vendors, and ZTE's bid was by far the lowest.

With no restrictions at the time on the use of ZTE equipment and facing several deployment challenges, our selection was a no-brainer. The choice we made not only enabled us to meet our mandated MF I buildout requirements, but also provided us with a reliable platform on which we could quickly deploy 4G LTE and VoLTE. Despite the challenges of our low density footprint, we were optimistic that this experience would allow us to provide the latest services to our community for the balance of the current technology generation, and also provide a solid foundation for the next.

Unfortunately, as the uncertainties have grown regarding whether we will be able to continue to use ZTE equipment, my optimism has greatly diminished. At a time when we should be focused on expansion plans and upgrades, we are, instead, concerned with whether we will be able to continue to provide any services at all. Such a fate would squander 20 years of network expansion and over $20 million in wireless investments. We find ourselves in this predicament more or less because under the Mobility Fund program, we simply did our best to do what the government required of us, to bring service to our neighbors.

With the news of the bills being discussed today, I can sincerely report that my optimism is returning. I am confident that by working with the small affected carriers, Congress and the appropriate Federal agencies will be able to establish reasonable and sound policies that provide the essential financial resources needed for those carriers to secure their networks.

The legislative efforts pending before this subcommittee take significant steps to plot a path to the future by establishing the Secure and Trusted Communications Network reimbursement program, determining a list of covered communications equipment or services, mitigating administrative burdens on small rural carriers, targeting network risk, and supporting information sharing. As Congress acts on these critical issues, it is important that solutions are implemented in a timely manner to support national security, they are executed in the right order to maintain services, and that sufficient resources are allocated to get it right.

With several efforts already underway, including through the executive order and pending proceedings before the FCC to prohibit use of covered equipment, there is no time to waste in funding the replacement equipment. And while many have referred to the process as rip and replace, I say that perhaps we really need to be talking replace and then rip. Otherwise, services will, indeed, be disrupted.

Finally, as Commissioner Starks noted in a public statement last week, this is a national problem that deserve a national solution, and we shouldn't expect small carriers who acted legally and in good faith to replace their insecure equipment on their own. It is, therefore, critical that Congress acts swiftly to provide resources for replacement of covered equipment, particularly for the small rural carriers who are unable to cover the cost without assistance. I believe the legislation before the subcommittee today accomplishes these things goals, and I applaud your work to legislate to secure our wireless future. I genuinely appreciate the opportunity to share a little of the story of my family's company, and I welcome any questions you may have.

[The statement of Mr. Nettles follows:]

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

Mr. Doyle. Thank you, Mr. Nettles.

Mr. Feld, you are recognized for 5 minutes.

STATEMENT OF HAROLD FELD

Mr. Feld. Chairman Doyle, Ranking Member Latta, thank you for inviting me here this morning. I applaud the subcommittee for moving forward with the set of bills designed to promote innovation and security in 5G networks. I want to focus on the following bills: The SHARE Act, the Network Security Information Sharing Act, the Secure and Trusted Communications Network Act, and the E-FRONTIER Act.

The SHARE Act. Everyone here is familiar with the problem of our increasingly crowded airwaves. Our efforts to find spectrum for 5G deployments have already caused conflict and uncertainty among Federal and commercial users. Investing in the development of spectrum sharing technology is a necessary investment to resolving these problems going forward.

In addition to research and sharing by Federal users with other Federal users, the study of the CBRS band will contribute enormously to our understanding of how to create a win for all spectrum users. The development process for CBRS balance the interests and concerns of multiple stakeholders, and has attracted early investment from licensed as well as unlicensed users, all while protecting Federal interests.

To meet our spectrum needs going forward, we need to set aside our old feuds and embrace systems that accommodate everyone and maximize spectrum use. The CBRS process tells us we can do it, and we should build on this success.

Importantly, we should not think about the SHARE Act as simply a means of freeing up more Federal spectrum for commercial use. The technologies developed should be seen as the first step in rethinking Federal spectrum management to move from the current stale and static system of specific assignments to a dynamic sharing system that allows the Federal Government to leverage economies of scale, and provide Federal agencies with the spectrums they need to meet their responsibilities.

NSIS and STCNA, these are both good ideas to address the critical issue of supply chain security in U.S. communications networks. With regard to the Secure and Trusted Communications Network Act, we have suggested slight modifications that would further clarify that there is a mechanism so covered entities that cured their supply chain security risk can be removed from the list. Although nothing in the statute as written prevents development of such a process, it is always best to clarify these things to avoid confusion.

We also suggest that the STCNA be expanded to include purchases made after August 2018 to ensure small carriers can be reimbursed for the purchase of equipment that was not listed at the time of purchase. Network security is a shared responsibility and benefits us all. These changes would affirmatively serve the public interest and protect national security. We look forward to continuing to work with the committee on these issues.

E-FRONTIER. It is often repeated that the most important rule of legislating is first, do no harm. The sweeping language used in the statute creates potential barriers to Federal provision of emergency communications services, or ways to leverage existing Federal assets in rural communities to address the digital divide. A proposal does not need to actually violate the law to cause delay or prevent needed action.

For example, if the Federal Government were trying to make Federal fiber

available to commercial carriers in the immediate aftermath of a natural disaster, no one would want to introduce delay and uncertainty while legal counsel debate whether this would be a wholesale network under the Act. There is no plan to build a national network of any sort, nor could any future administration do so without an appropriation from Congress. Given that enactment of E-FRONTIER provides no additional benefit to offset the risks of unintended consequences, we strongly recommend that this bill not move forward.

Thank you very much. I look forward your questions.

[The statement of Mr. Feld follows:]

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

Mr. Doyle. Thank you very much.

Mr. Brenner, you are recognized for 5 minutes.

STATEMENT OF DEAN R. BRENNER

Mr. Brenner. Chairman Doyle, Ranking Member Latta, and members of the subcommittee, my name is Dean Brenner, and I am here today on behalf of Qualcomm, which was founded in a San Diego living room but is now the world's largest supplier of chips, an entire modem RF system for smartphones and other wireless devices, and the world's leading inventor and licensor of new wireless technologies.

The technologies we develop, especially 5G, and the chips we design, all depend on one key input controlled by the government: spectrum. As this subcommittee has recognized, enabling a steady stream of new spectrum, low, mid, and high band, licensed, unlicensed, and shared, is essential for the rapid broad 5G rollout. We are working on 5G at a feverish pace, but our work depends on the continued steady stream of new spectrum, so thank you for continuing to make spectrum a high priority.

5G has now launched on four continents. More than 30 5G networks, including those of all four U.S. national operators, have launched and are expanding. Over 20 manufacturers are selling or developing 5G devices, more than six times as many as in 4G's first year. Qualcomm's chips are in more than 150 5G devices which have been or soon will be launched including phones, hot spots, and fixed wireless devices. Our chips support both sub-7 gigahertz and millimeter wave, and the U.S. was the first country to launch 5G in both sub-7 gigahertz and millimeter wave. 5G is delivering far better mobile

broadband at a much lower cost per bit. Let me explain several 5G game changers which will launch soon and will further accelerate the 5G rollout.

Dynamic spectrum sharing, or DSS, enables an operator to run 5G in spectrum already in use for 4G. Instead of having to empty a 4G spectrum band before launching 5G, which could take 10 years or more, DSS will enable a band to be used simultaneously for both 4G and 5G. Enhanced millimeter wave will enable 5G fixed wireless to be used for rural broadband. Qualcomm has developed new antenna modules which enable 5G fixed wireless service 1 mile away from a rural base station, covering a much larger area than anyone thought possible.

A new version of 5G, optimized for unlicensed spectrum, will enable 5G to be launched for ultra low latency, ultra reliable 5G in factories, warehouses, and other venues. This technology, along with new forms of WiFi that Qualcomm is developing, will be deployed in new 6 gigahertz unlicensed spectrum now under consideration by the FCC. Qualcomm's 5G small cell chips will expand 5G to more people and more locations, particularly indoors using millimeter wave.

Last, cellular vehicle to everything or C-V2X technology, first with 4G and then 5G, enables cars to communicate with other cars and infrastructure with much greater range and reliability that is possible with older DSRC technology. For C-V2X to be it deployed, the FCC must waive or change its rules for 5.9 gigahertz, which only allow deployment of DSRC.

Let me turn to 5G security, which has been a high priority for Qualcomm ever since we started working on 5G even though we don't manufacture core network equipment. Qualcomm has worked on 5G security internally with many other companies, and in the 3GPP global standards group, which sets 5G standards.

In addition, for many years now, Qualcomm has been an active participant and leader in CSRIC, the FCC's Communication Security Reliability & Operability Council. Most recently, we appreciated the bipartisan May 9 letter sent from the chairman and ranking members of this subcommittee and the full committee to FCC Chairman Pai asking that CSRIC examine 5G security.

Subsequently, one of our engineers, Dr. Farrokh Khatibi, was appointed to lead the CSRIC working group on managing security risks and emerging 5G implementations. The members of this group include experts from DHS, a county government, a non-profit, government contractors, network operators, tech companies, standards groups, and a trade association. We look forward to advancing 5G security through this group.

Finally, Qualcomm has been working on spectrum sharing for many, many years. We have worked directly with NTIA, DoD, and other government agencies as well as with private sector colleagues. Often, a spectrum band analyzed for sharing involves multiple cabinet departments and multiple entities in those departments.

Over the years, NTIA has played a coordinating role of gathering technical input from government players, working with industry, leading joint public/private technical work, and speaking with a single voice for the executive branch to make to make greater progress toward sharing. This process culminated most recently in the initial commercial deployments in the CBRS band, a great development to increase the amount of mid band spectrum for 4G and 5G.

We are very pleased with the heightened interest in sharing across the Federal Government, and we look forward to continuing to work through this process to enable more intensive spectrum sharing. Thank you very much, and I look forward to your questions.

[The statement of Mr. Brenner follows:]

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

Mr. Doyle. Thank you, Mr. Brenner.

So we have concluded our openings. We now move to member questions. Each member will have 5 minutes to ask questions of our witness. I will start by recognizing myself for 5 minutes.

Ms. Stempfley, what risks are being posed by untrusted equipment in our Nation's telecommunications networks, and what kind of things can hostile foreign actors do if they have access to that equipment?

Ms. Stempfley. I want to thank you for the question. So as I said in my testimony, the telecommunications infrastructure provides great interconnectivity, and actually serves as the foundation of many other -- many elements of life. It also has cascading dependency with other physical infrastructures, and, therefore, presents a key area of focus.

The supply chain concerns are equally within that -- are difficult to identify, and could provide a great deal of access not just to the environment, the services provided, but the management infrastructure underneath. So I think it goes without saying that they are of great concern for us to understand.

Mr. Doyle. Yeah. I mean, we have heard reports that hostile foreign actors are accessing our Nation's electrical grid and infrastructure. I mean, what other critical sectors could they access if they accessed a carrier's network through compromised equipment?

Ms. Stempfley. Sir, unfortunately, the work that we do at CERT couldn't give you a clear answer to that activity. The piece, though, that I think we all understand is the telecommunications infrastructure, the electric sector, the financial sector are all interdependent. I think that speaks to the potential cascading effects.

Mr. Doyle. Mr. Feld, tell me, what are the benefits of establishing a strategy for the Federal Government to develop these test beds for more efficient spectrum sharing, and what benefits do you see applying the lessons we learned in the CBRS band and other Federal bands?

Mr. Feld. Thank you. The need for more sharing is obvious, but the benefits of sharing go beyond simply ensuring that the Federal Government can maintain its current functions. The dynamic spectrum sharing and other technologies that Mr. Brenner referred to allow the Federal Government potentially for the first time to act as a single spectrum user, rather than atomizing spectrum allocations in our current system.

Additionally, the CBRS band demonstrates the importance of accommodating Federal users, licensed protected users, unlicensed users, which has been the holy grail of spectrum policy. The ability to let everybody do what they need to do and what they want to do is the ultimate goal of spectrum policy, and these sharing technologies will make that possible.

Mr. Doyle. Thank you, Mr. Feld.

Mr. Nettles, how do you see the Network Security Information Sharing Act

benefiting your company going forward and mitigating risk to your supply chain?

Mr. Nettles. Thank you, Mr. Chairman. It would be of tremendous benefit to us. We are a pretty small company. We have 50 employees to cover all lines of business, about half of which are dedicated to our wireless network. I mean, it is difficult, to say the least, to keep up with technology coming out, and when it is not shared openly, you don't know what you don't know. It is not that many crossroads, unfortunately, and that is kind of where we found ourselves a few years back in our ZTE selection.

Mr. Doyle. Yeah. Ms. Stempfley, do you believe the Network Security Information Sharing Act that I have introduced with Representative Kinzinger will help our smaller telecom providers receive important information related to supply chain security threats, and what are the challenges that you have seen in communicating these types of threats to companies that don't have the resources and personnel of a tier one carrier?

Ms. Stempfley. I think the focus on ensuring that information is actionable and usable to all parties is a really important part of the bill, and of any information sharing related program. And so, the key thing that we have found, that I have found in building these sharing activities is recognizing the capacity that the organization has to take action. So is it clear what they should do, and is it communicated to them in a language and in a method they can actually physically receive it in?

Mr. Doyle. Thank you very much.

I am going to yield 25 seconds back as an example for the rest of the committee. I now yield to my good friend, Mr. Latta.

Mr. Latta. Thank you very much, Mr. Chairman, and again, thanks to our witnesses for being with us today.

Mr. Brenner, if I could start my questions with you, please. The U.S. wireless

industry has prospered due to market-based technological innovations and policies that incentivize growth. We have led the way with spectrum auctions in the early 1990s, and more recently, with the successful AWS 1 and 3 auctions. How important are the tools given to NTIA in the SHARE Act for continued U.S. wireless leadership over the next decade?

Mr. Brenner. So thank you for that question, Congressman Latta. The tools are vital, but I would suggest -- so the list of the tools which is Section 106(b)(2)(b) of the bill needs to be added to include two more, and let me explain them.

The first we call "look before talk." So today, the way an unlicensed channel would be shared, if the four of us on this panel were sharing, I would get to use it one-fourth of the time, and I would have to be quiet the other three-fourths; the same for Mr. Feld, same for Mr. Nettles, same for Ms. Stempfley. But with 5G, we have this fast new radio, and we are transmitting in highly directional manner, and we have demonstrated this technology.

As long as all four of us on the panel, each are able to detect in what direction the other is going to be using the spectrum, all four of us could use the spectrum at once, thereby dramatically increasing the utilization for everyone. So we call that "look before talk." The technical name for it, I apologize, is coordinated multi-point.

The second tool that is vital is synchronization. So if we all synchronized our watches while we were sharing the channel, because of the time-based aspect of spectrum sharing, if we were in sync with one another, we would minimize the amount of time, of dead time on the channel, and again, all of us would be able to use the channel more, which would be a benefit to everyone.

Mr. Latta. Thank you very much.

Ms. Stempfley, with your prior experience in the Office of Cybersecurity and Communications at the DHS, would you discuss how H.R. 4461 would function in the system with existing executive branch workrooms to facilitate information sharing with small rural providers?

Ms. Stempfley. Yes. Thank you very much. I truly appreciate the focus on the small rural provider-related activity. It is an important part of our Nation's infrastructure, the tier. Within the information sharing programs that exist, sharing typically happens between a government entity with a consolidated group, whether it be an ISAC, or a trade association, and then the information is further disseminated from there. I think the way that this bill would work would be to ensure that the complete path exists and is successful, so that the end provider not only can receive the information, but then can provide the feedback back into the government that the full set of activities has occurred, and I appreciate that in the bill.

Mr. Latta. Thank you. Let me follow up with another question. H.R. 4459 calls for disposal of suspect equipment. Do you have any concerns about this equipment being resold on the secondary market? And just also, and from a technological perspective, could this equipment be sanitized and resold, or should we just destroy it entirely?

Ms. Stempfley. There are many nuances within your question, sir, so I appreciate the depth of it. There is, I think, always a concern. If you listen to the many areas you must address in the supply chain from relationship management to engineering to operations practices, there is always a concern that equipment that is vulnerable could be used in another place, and that should be addressed directly, and so the idea of how to either sanitize or destroy the equipment is an important question.

It is unclear whether it will be sanitizable. It really depends on what the risk

within the supply chain that you are dealing with. In some instances, you can do something as simple as change software or firmware. In other instances, it can be more profound as an engineering flaw, and that would need a greater, a more severe response.

Mr. Latta. Let me just follow up real quickly with that, because when you are talking about, you know, how one would be able to do it, what would be the expertise that one would have to have to be able to make sure that it is totally sanitized, then?

Ms. Stempfley. I believe you would need both network expertise, security, cybersecurity expertise, and some level of software programming, software and hardware programming expertise in order to ensure it.

Mr. Latta. Thank you.

Mr. Chairman, I yield back the last 17 seconds and also submit my questions to the witnesses to be answered later. Thank you.

Mr. Doyle. Thank you, Mr. Latta. Another good example from the leadership of the committee.

Mr. McNerney, you are recognized for 5 minutes.

Mr. McNerney. I thank the chairman for his leadership here, and I thank the witnesses.

Mr. Nettles, I represent a district that has a lot of rural areas, and I believe that the wireless carriers would agree with you about the need for additional resources to replace some of this equipment. Do you think that the high cost program under the universal service fund has contributed to these problems, and if so, could you explain that a little?

Mr. Nettles. I most definitely think it contributed to it. The direction seems a little bit askew to the policy objectives of providing the most service to as many people everywhere as you can, the areas that are generally the least or most underserved, those

that lack economies of scale, and so, you know, the abandonment of the notion of a rate of return seems a little bit counterintuitive or backwards.

So, you know, to say what is the least amount of money -- you know, I want you to go serve this area that is already uneconomical to serve for the least of amount of money that you will take to do it just doesn't quite add up to me.

Mr. McNerney. Thank you.

Ms. Stempfley, it is clear that a major factor in the problems we face today is the cheapest equipment has led to the equipment with the weakest security, and we are just seeing that over and over. How do we go about ensuring that in the future that equipment is more affordable, the secure equipment is more affordable?

Ms. Stempfley. You have hit upon one of the most difficult challenges in security, and that is, trying to ensure that we understand what security requirements exist and we engineer them in from the beginning. We talk a lot about the fact that organizations have accepted a security debt. That debt is handed to them when they purchase insecure components where security was not considered from the beginning. So, bringing those requirements into the engineering and design phase is the most important way to increase --

Mr. McNerney. That could make us, our equipment more competitive with, say, Huawei and ZTE. Thank you.

Do you agree, Mr. Feld?

Mr. Feld. Yes. I think the problem here is as other people have focused the economies of scale and the ability of foreign --

Mr. McNerney. Would you talk in the microphone a little bit?

Mr. Feld. Sorry. Yes. I agree that the cost is a big concern. We need to make sure

that security is affordable for everyone, and if we do not take steps to try to equalize the playing field for countries like China that can subsidize insecure equipment, or have their own economies of scale, ultimately, it is consumers that will pay the cost either needing to buy higher-priced equipment, or from insecure networks.

Mr. McNerney. Earlier you were singing the praises sharing spectrum -- spectrum sharing among Federal users as well as non-Federal users. Are there opportunities for this model to work elsewhere, for example, between commercially licensed and unlicensed users?

Mr. Feld. I believe there are a lot of opportunities that can be explored here. One of the important elements of CBRS is called user share, which means if the licensed provider is not actually using the spectrum capacity in an area, then somebody else can. When the licensee is ready to deploy, then the unlicensed equipment will stop working because of the spectrum access system. So the spectrum can be in productive use all the time, and the license provider can decide when it is appropriate to deploy, but we don't have to have rural areas captive to buildout in the urban areas first. We can have local providers deploy using the sharing concepts.

Mr. McNerney. Well, why isn't sharing enough spectrum for unlicensed services would help close the digital divide? How can that help close the digital divide?

Mr. Feld. Well, we have a number of local providers who are small businesses, wireless ISPs, or WISPs, who use right now the unlicensed spectrum to provide because that equipment is affordable and available, and because they are in areas that the larger licensed carriers simply don't want to serve. They don't provide enough rate of return. But these guys who are actually part of the community and small businesses can make it work if we allow them to make it work. Giving them access to this additional spectrum

capacity will be a huge boost in their ability to provide service in these rural areas.

Mr. McNerney. And before I close, I just want to make a plug for the Digital Equity Act which I just introduced yesterday and broadband adoption.

Mr. Feld. And which we publicly acknowledge and thank you very much and fully support.

Mr. McNerney. Thank you. I yield back.

Mr. Doyle. The gentleman yields back.

The chair now recognizes the ranking member of the committee, Mr. Walden.

Mr. Walden. Mr. Chairman, thank you, and thanks again to all of our witnesses.

Mr. Nettles, H.R. 4459 calls for the reimbursement program to be completed within a year. With your staffing and the funds suggested in the draft, how confident are you that you could replace all your ZTE equipment in that timeline?

Mr. Nettles. Mr. Walden, thank you for that question. It is going to be a challenge. There is no other way to put it. A year -- you know, I guess it is sort of -- in part, sort of depends on when is day zero in that process. You know, if we have got -- I believe there was also a provision that gave the FCC up to a year to establish what was actually on the equipment. At this stage of the game without knowing, you know, which of the components within the network actually will have to be replaced, it would be difficult -- if it involved both the RAN and our core, I would say it is virtually impossible to do it within a year without just a concentrated effort from suppliers, you know, the --

Mr. Walden. Do you think there would be equipment shortages, labor shortages? I mean, we have been through a couple of these types of transitions, you know, with the repack, broadcasters and all, and you give them 39 months, and everybody rushes out to get it done.

Mr. Nettles. Labor shortages would probably be the most probable situation.

Mr. Walden. Right. If we aren't able to address this uncertainty and provide relief to providers, especially when they use Mobility Fund I money to build the network, what could happen? What should we be aware of? Could this lead to a loss in 911 coverage in some areas if providers like you are the only provider in that area?

Mr. Nettles. Most definitely. I mean, if we are required to rip it out first and then put in the replacement equipment, I mean, it is -- without sounding, you know, it would be like selling your car before you buy your new one. You are going to be walking.

Mr. Walden. Got it.

Mr. Brenner, I want to come to you with a question on spectrum management, H.R. 4462, the SHARE Act. As a company that sees every angle in this whole wireless debate from licensed spectrum used in 5G to the unlicensed spectrum that will offload a lot of traffic to the shared spectrum of Federal users, how important is it that NTIA have full visibility and control over Federal access to spectrum in order to gain the most efficiencies while still meeting the missions of the agencies?

Mr. Brenner. Thank you for that question, Congressman Walden. It is extremely important. You know, NTIA was created in the late 1970s because each Federal agency just had their own spectrum system, and there was no single coordinator. But you know, for sure we would not have been able to achieve the success with the CBRS band without having NTIA play that role.

Now, as you mentioned, you know, as Qualcomm, we work with everyone. As I mentioned in my testimony, it is great to hear that the Defense Department really has a revolutionary attitude about spectrum sharing, but these are very complicated situations. So in the two bands that are mentioned in the SHARED Act, one of them, 7 gigahertz, has

8,700 Federal assignments of spectrum. The 3.1 to 3.5 band has 450 assignments of spectrum. So NTIA, in August, sent a memo to the Federal agencies. Tell us. We have got all these assignments. Who is actually using the spectrum? So there has to be a single voice. It has to be NTIA.

Mr. Walden. A clearinghouse. Somebody overseeing it, yeah. And I won't put you on the spot. I don't have to.

You know, we are in this bit of a struggle right now where DoD, at least allegedly, wants to grab more control over management of spectrum, and some of us believe that is sort of an agency grab away from NTIA. We witnessed this in the last Congress when they wanted to avoid FDA approval of drugs and medical devices for battlefield needs because they were irritated with the slowness in one approval of one product, which we got resolved, but they wanted to go be their own FDA, and I just think it is bad public policy.

You don't have to respond to that because you work with all of them. But I think we are -- if there is a couple things that brings us together as Republicans and Democrats on this subcommittee, this is one of them, a couple of them, and so it is something we care a lot about.

Finally, you know, Mr. Chairman, in light of the votes on the floor coming, I will yield back. But again, thank you to all of you for your testimony. It is most helpful.

RPTR BRYANT

EDTR ROSEN

[10:29 a.m.]

Mr. Doyle. I thank the gentleman.

Mr. Veasey, you are recognized for 5 minutes.

Mr. Veasey. Mr. Chairman, thank you very much. I really appreciate it, and happy that we are here today to talk about this very important subject. I would like to thank our witnesses for coming here to share your experiences and expertise as we talk about this very critically important infrastructure, this wireless infrastructure that is really important for our future.

And I wanted to ask Ms. Stempfley, in your testimony you discuss the need to manage risks across the entire global chain regarding wireless infrastructure, including manufacturing and integration supply chains.

Currently, the only other major suppliers of 5G networking equipment are Huawei, ZTE, Nokia, Ericsson, and all of those are foreign companies. As I understand it, there are no major U.S. producers of this telecom technology.

The Secure and Trusted Communications Networks Act will mandate that no Federal funds can be used for communications equipment and service that pose an unacceptable risk to national security. Given that language and the lack of U.S. producers of telecom equipment, what manufacturer can we use to ensure that we won't face the same issue later after the risky equipment has been removed and replaced?

Ms. Stempfley. Sir, I appreciate the question. Unfortunately, that is not really my area of expertise, and I could only speculate. I regret that I am not in a position to talk about the suppliers in the market.

Mr. Veasey. Are there any -- and anybody can answer this one. Are there any U.S. producers of this telecommunications equipment that can pick up the slack that will be created in the market by prohibiting certain foreign made products; and, if so, how long do you think it would take for that producer to create enough infrastructure to replace all the equipment that is contemplated being replaced?

Mr. Nettles. If I may, I will go back to the answer I gave just a few minutes ago, sir. It kind of sort of depends on what -- well, not kind of sort of. It absolutely depends on what we have to replace. If we have to replace the radios and the core, that is one order of magnitude. If it is just the core, that would be a little more manageable, including the ability to rehome our networks to, you know, existing cores that are in place from an infrastructure sharing standpoint.

There are some niche vendors in the U.S. that make parts, you know, parts of the network. One of the challenges a small company like we have, you know, is when you buy components from different vendors, it adds a level of complexity in making everything work together that makes it almost unmanageable.

It is my understanding that as far as the major vendors, Nokia and Ericsson, and even Samsung has been one that has been mentioned as one that would, based on a democratic country, would be one that would be considered a favored equipment or favorable.

Mr. Veasey. In your testimony, you discuss the challenges of providing wireless service to rural communities and the cost considerations of certain wireless equipment over others. You also discussed the concerns about the ability of small providers, and to make upgrades to facilitate next-generation services in rural areas.

Could you give me your opinion regarding whether the provisions in the Secure

and Trusted Communications Networks Act would substantially delay 5G and other wireless deployment to unserved and underserved communities?

Mr. Nettles. Would it delay? No, sir. I think it would make it -- it would make it even more possible. Right now, I am looking at, you know, do I even try to stay in the business or do I just, you know, get what I can for it and walk away.

Mr. Veasey. Thank you.

Mr. Chairman, I yield back.

Mr. Doyle. I thank the gentleman.

The chair recognizes Mr. Johnson for 5 minutes.

Mr. Johnson. Thank you, Mr. Chairman. I appreciate the hearing.

Mr. Brenner, as you know, the SHARE Act calls for the establishment of an integrated spectrum automation enterprise strategy with at least one testbed to facilitate the sharing of spectrum by more than one Federal entity.

Can you touch on the importance of establishing a sharing test bed? What are some of the potential consequences if the FCC and NTIA don't require this capability before Federal entities attempt to share the same spectrum space?

Mr. Brenner. Thank you, Congressman, for that question. So at Qualcomm, we constantly, aggressively, 24/7, we have tests going on of new technologies all over the place, largely on our campus in San Diego, but also around the world.

So our whole business is inventing new technologies and testing and testing and testing them, to make sure that they are going to work, to convince providers like Mr. Nettles that they are beneficial to be deployed, to convince equipment vendors to deploy them.

And so that is the approach that has been successful to establishing United States

leadership in the wireless space; and having that same kind of capability occur so that the testing can occur on the Federal side, I would say would be vital.

Mr. Johnson. Well, you gave a good explanation of why it is important, but what happens if we don't do that? What are the consequences if the FCC doesn't require this capability before Federal entities attempt to share that same spectrum space?

Mr. Brenner. Right. So the FCC can't require Federal entities to do testing. So that is point number one. Point number two, if no one else -- the FCC, as an independent agency, has no authority over the executive agencies.

But second of all, if you don't have that capability in the executive agencies, then what you have is what we have had for the last several decades, which is the Federal Government continues to use old legacy systems, and they don't have a modern wireless communications capability that we have in the commercial sector. That is bad in and of itself.

And then the second thing that leads to is then when we want to have sharing, it becomes extremely difficult, because the commercial sector has state-of-the-art technology whereas the Federal Government has older legacy systems that were never designed for sharing.

Mr. Johnson. Okay. Mr. Feld, do you have any thoughts on that?

Mr. Feld. Yes. I completely agree with everything Mr. Brenner said. I also want to stress that the enormous opportunity here for the Federal Government to leverage its vast economies of scale requires that there be this focused central testing. Somebody has to be responsible for making it happen, and it can't be left to the vagaries of agencies.

We need to understand that for most agencies, they are not interested in spectrum policy. They are trying to get their mission accomplished, and they are trying to

do it within budgets for which upgrading of equipment or testing equipment is simply not an element. So there is no reason to believe that these things will happen without a statutory mandate to make it occur.

Mr. Johnson. Ms. Stempfley, in your testimony, you talked about the importance of having a full view of the dependencies and complexities of supply chains as they change moving into the future. What role does or should NTIA continue to play coordinating a software or hardware bill of materials?

Ms. Stempfley. I would like to commend NTIA for the work that they have been doing on the software bill of materials. In our experience in handling risks, particularly software-oriented risks that exist, we have found that the software bill of materials is possibly the most effective way to understand the complexities and the nested nature of all of the technology that exists in place.

And it provides a foundation to integrate software bills of material with other hardware bills of material and multimodal bills of material, and would like to continue to see NTIA play a leadership role within the government on this topic.

Mr. Johnson. Thank you, Mr. Chairman. I beat you, I gave back 35 seconds. I yield back.

Mr. Doyle. The chair now recognizes Mr. Soto for 5 minutes.

Mr. Soto. Thank you, Mr. Chairman.

The House Permanent Select Committee on Intelligence has stated that China has, quote, "the means, opportunity, and motive to use telecommunications companies for malicious purposes," unquote. By a show of hands, how many of you agree with that assessment? Interesting.

Mr. Nettles. I am sorry, I missed the question.

Mr. Soto. So the question again is: The House Permanent Select Committee on Intelligence has stated China has, quote, "the means, opportunity, and motive to use telecommunications companies for malicious purposes." Please raise your hand if you agree with that statement. Okay.

It would be great to hear first from, then, Mr. Brenner on why you disagree with that statement.

Mr. Brenner. Yes. Congressman, thank you. It isn't that I disagree with the statement or agree with the statement. I don't have any information about China as a country, their capabilities to infect our communication system. I obviously would think that would be a horrible thing, and I think that the U.S. Government should do everything at its disposal to make sure that doesn't happen.

But when you say China, another reason I didn't raise my hand is Qualcomm, we sell chips to vendors. Some of them are Chinese vendors, and they are deploying our chips in phones in China. And I have no information -- I think that is a very good thing for U.S. leadership.

And I have no information, obviously, that there are any security issues in any of our chips, but, obviously, I completely share the concern. If China has a capability to harm the United States, I want the United States to do everything they can to prevent that.

Mr. Soto. Ms. Stempfley, what is your opinion on that statement?

Ms. Stempfley. I believe that there are a number of security risks within the infrastructure and that we should do everything we can to reduce them and to make it more difficult for anyone who has means, motive, and opportunity to take advantage of those.

Mr. Soto. Thank you. There has been a growing movement within Congress, whether it is in the National Defense Authorization Act or in other major bills, to encourage national foundries, to encourage manufacturing of high-tech equipment here in the United States. In my district, we have the Bridge Project, which is creating tamper-proof sensors.

Mr. Feld, how critical is it that we continue to develop national foundries here to develop next-generation technology in the telecommunications industry and beyond?

Mr. Feld. Well, I think we in the United States have a long tradition of our leadership in this area. We want to maintain that, obviously. I think that it is very important, and that just as government had a role in fostering the creation of the internet and in fostering the development of many technologies in which we now have a leadership role, I think that there is a role for policy and encouraging these sort of foundries as well.

Mr. Soto. And then, we have a bill with Congressman Flores, H.R. 575, which is encouraging, with the development of 5G, to adopt the Prague 5G security recommendations. How many you all, by a show of hands, agree that we should be adopting the Prague 5G security recommendations as we develop 5G in this Nation? Please raise your hand. Okay.

I noticed, Ms. Stempfley, you didn't. Please give us your opinion on that.

Ms. Stempfley. I am not familiar enough with the details of it in order to speak intelligently.

Mr. Soto. Sure.

I am going to yield back now. Thank you, Mr. Chairman.

Mr. Doyle. I thank the gentleman.

So we have multiple votes on the House floor which could keep us down there an hour, or maybe a little bit longer. We have polled the membership on both sides to see if they are comfortable with waiving their 5 minutes for questions.

So if I don't hear any objections from either side, I would like to ask unanimous consent to enter the following documents into the record: An article from zero5g.com referenced earlier by Ranking Member Walden, a flier regarding 5G referenced earlier by Ranking Member Walden, a letter from the International Associations of Fire Chiefs. Without objection, so ordered.

[The information follows:]

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

Mr. Doyle. I want to thank all the witnesses for their participation in today's hearing. I want to remind members that, pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared, and I would ask each witness to respond promptly to any such questions you may receive.

At this time, the subcommittee is adjourned.

[Whereupon, at 10:42 a.m., the subcommittee was adjourned.]