LEGISLATING TO SECURE AMERICA'S WIRELESS FUTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 27, 2019

Serial No. 116–67

Printed for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

47–352 PDF WASHINGTON : 2022

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
DIANA DEGETTE, Colorado
MIKE DOYLE, Pennsylvania
JAN SCHAKOWSKY, Illinois
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
JERRY MCNERNEY, California
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
PAUL TONKO, New York
YVETTE D. CLARKE, New York, *Vice Chair*
DAVID LOEBSACK, Iowa
KURT SCHRADER, Oregon
JOSEPH P. KENNEDY III, Massachusetts
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona

GREG WALDEN, Oregon
Ranking Member
FRED UPTON, Michigan
JOHN SHIMKUS, Illinois
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY MCMORRIS RODGERS, Washington
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. MCKINLEY, West Virginia
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
LARRY BUCSHON, Indiana
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GREG GIANFORTE, Montana

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
MIKE BLOOMQUIST, *Minority Staff Director*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MIKE DOYLE, Pennsylvania
Chairman

JERRY MCNERNEY, California
YVETTE D. CLARKE, New York
DAVID LOEBSACK, Iowa
MARC A. VEASEY, Texas
A. DONALD MCEACHIN, Virginia
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California, *Vice Chair*
PETER WELCH, Vermont
BEN RAY LUJAN, New Mexico
KURT SCHRADER, Oregon
TONY CÁRDENAS, California
DEBBIE DINGELL, Michigan
FRANK PALLONE, JR., New Jersey *(ex officio)*

ROBERT E. LATTA, Ohio
Ranking Member
JOHN SHIMKUS, Illinois
STEVE SCALISE, Louisiana
PETE OLSON, Texas
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
BILL FLORES, Texas
SUSAN W. BROOKS, Indiana
TIM WALBERG, Michigan
GREG GIANFORTE, Montana
GREG WALDEN, Oregon *(ex officio)*

C O N T E N T S

[1] The information has been retained in committee files and also is available at https://docs.house.gov/meetings/IF/IF16/20190927/109991/BILLS-116HR2063ih.pdf.

[2] The information has been retained in committee files and also is available at https://docs.house.gov/meetings/IF/IF16/20190927/109991/BILLS-116HR2881ih.pdf.

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, DC.

The subcommittee met, pursuant to notice, at 9:28 a.m., in the John D. Dingell 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, Cárdenas, Pallone (ex officio), Latta (subcommittee ranking member), Shimkus, Kinzinger, Bilirakis, Johnson, Long, Flores, Walberg, Gianforte, and Walden (ex officio).

Staff present: A. J. Brown, Counsel; Jeffrey 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 and Technology; Margaret Tucker Fogarty, Minority Legislative Clerk/Press Assistant; Peter Kielty, Minority General Counsel; Bijan Koohmaraie, Minority Deputy Chief Counsel, Consumer Protection and Commerce; Zack Roday, Minority Communications Director; and Evan Viau, Minority Professional Staff Member, Communications and 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.

OPENING STATEMENT OF HON. MIKE DOYLE, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

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 ONTIER Act, introduced by Representatives Cárdenas 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 were 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.

[The prepared statement of Mr. Doyle follows:]

PREPARED STATEMENT OF HON. MIKE DOYLE

Today, we are considering a series of bills to secure America's wireless future. They will ensure that the Government manages the federal and commercial spectrum more efficiently to promote innovation and better serve all Americans. They also will 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 in introducing the SHARE Act. Their bill will cement the long-standing policy that our nation's key agencies-the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC)—remain responsible for spectrum policy. These expert agencies can act as impartial judges to balance the demands and interests 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 the 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. 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 Citizen's Broadband Radio Service.

When it comes to securing these networks from foreign adversaries, I want to thank Ranking Member Walden, 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 one-billion-dollar 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 anyone 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 networks 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.

Representative 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.

I look forward to hearing from our witnesses. I also want to briefly recognize Dean Brenner, on today's panel, who is a fellow Monmouth County, New Jersey native. Welcome.

The Chair recognizes Mr. Latta, ranking member of the subcommittee, for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. ROBERT E. LATTA, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. LATTA. Well, thank you very much, Mr. Chairman, and thank you very much for calling today's hearing; 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 the spectrum and telecommunication matters, NTIA should continue to play the lead role in 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 address vulnerabilities in our Nation's communication networks, such as the inclusion of unsecured 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 come 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 cyberattacks 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.

[The prepared statement of Mr. Latta follow:]

PREPARED STATEMENT OF HON. ROBERT E. LATTA

Welcome to today's subcommittee hearing to discuss legislation that seeks to address our network supply chain security and management of our spectrum resources. Thank you to our witness panel for being here.

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'm especially pleased to have worked with Chairman Doyle on H.R. 4462, the SHARE Act, to empower our agencies to facilitate innovative spectrum sharing strategies to more efficiently using our airwaves. As the executive branch agency principally responsible for advising the President on spectrum and telecommunications matters, NTIA should continue to play the lead role in directing a collective government approach to managing the Federal Government's access to spectrum resources. This bill helps empower NTIA to use new tools to meet the challenge of growing wireless needs in the 21st century.

Today's hearing also features several bills to address vulnerabilities in our nation's communications networks, such as the inclusion of unsecure equipment. Many providers' networks contain gear supplied by suspect foreign carriers; however, this is only because the provider didn't understand the associated risks. The bills before us seek 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 also voiced concerns about network security and proposed prohibiting USF recipients from using controversial equipment. So, Fund II reverse auction comes to grips with the buildout requirements accompanying these funds; it is critical that we work in a bipartisan way to ensure they can revisit how those conditions impact their winning bid in order to keep their equipment free from security vulnerabilities. Not only do we want to prevent 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.

Thank you again to our witnesses for being here, and with that, I yield the remainder of my time to my friend from Illinois, Mr. Kinzinger.

Mr. DOYLE. The gentleman yields back.

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

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

Mr. PALLONE. 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 the 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 interests 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 the 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.

[The prepared statement of Mr. Pallone follows:]

PREPARED STATEMENT OF HON. FRANK PALLONE, JR.

The topic of today's hearing is important because not only must we ensure that we allocate our federal spectrum in ways that match our Government's future wireless needs, but we must also ensure that once those allocations are set, those systems are secure. One way that we can make sure that we have appropriately allocated our nation's airwaves to their best and highest uses on the federal side is to keep pushing ourselves to explore ways to use them more efficiently. Part of that effort must be improving our sharing technologies to advance and become more efficient and versatile.

We have made great strides, even just this year, on spectrum sharing. For example, we need to look no further than the 3.5 gigahertz band, which now has a novel three-tiered sharing system in place that allows federal and non-federal users to share a single band, and according to the FCC, will soon have a spectrum auction that will, for the first time, make mid-band spectrum available for 5G.

Another great example is the TV white spaces in the 600 megahertz band, which were freed up for unlicensed use in the Broadcast Incentive Auction. The creative thinking that went into that innovative allocation made prime low-band spectrum available for sharing-possibly a critical component of our 5G future.

Today, we're going to talk about how we can do more creative thinking on the federal side. Led by the capable folks at NTIA, I am confident that we can continue to push the envelope on finding new and innovative ways to share this valuable federal resource.

As I've said before, spectrum is a bipartisan issue. The work we are doing in this Committee today will help pave the way to a spectrum-rich future where spectrum "crunches" is a thing of the past.

But, the full measure of any progress we make in increasing connectivity and opportunity on our airwaves can only be realized if American consumers and businesses can count on secure and reliable service, which is why the Committee has been hard at work on legislation to secure the nation's networks.

I want to thank Ranking Member Walden, Congresswoman Matsui, and Congressman Guthrie for partnering with me to introduce one of the bills we're discussing today, the Secure and Trusted Communications Networks Act. This bill establishes a reimbursement program under the FCC to help communications providers cover the costs of removing compromised equipment from their networks and installing more secure alternatives in its place.

Much of the global supply chain for telecommunications equipment and services 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 anywhere else. Although some of the larger providers have known about and avoided these threats for some time, it remains a major issue for smaller and more rural carriers who built their networks using Huawei equipment.

This Committee recognizes there's a premium on security and that it's a premium worth paying. I look forward to hearing from our witnesses about how our bill helps providers ensure their networks are built with the most secure and reliable equipment available.

I also want to commend the Ranking Member of the Subcommittee, Congressman Latta, for partnering with Chairman Doyle on another bill before us today, which aims to modernize and expedite how the Government disseminates important security information to trusted communications providers.

I look forward to continuing this work with my friend from Oregon as we move ahead on these important measures, and I thank the witnesses for being here to help us in that process.

I yield back.

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 six 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. Mr. Pallone 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.

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

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. 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 two 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. 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 out on 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 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 the stories is about 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 risks from 5G. And that 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.

[The prepared statement of Mr. Walden follows:]

PREPARED STATEMENT OF HON. GREG WALDEN

Thank you, Mr. Chairman. I want to welcome our witnesses to this hearing. Your insight will be another important input in the process we began last Congress to secure our communications networks.

Our nation's telecommunications infrastructure represents the lifeblood of preserving a free and open society, 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 to have a bipartisan process to mitigate these threats and 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 communication networks from vulnerable equipment. In fact, we heard testimony over two years ago on the vulnerabilities that may exist in our networks. We have 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 within their budgets, not to mention within Federal programs' purchasing guidance to deploy the most effective products. Unfortunately, our adversaries have no reservations about subsidizing their pet companies and thus become attractive options for the budget sensitive providers.

I've 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 the most constituents in some of the hardest to reach places. Many of these providers don't have an army of consultants with the necessary security clearances to understand what vulnerabilities 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, "well, not that lowest cost equipment."

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 last Congress, and I'm pleased to see this concept at today's hearing.

H.R. 4459, the Secure and Trusted Communications Networks Act, of which I am an original cosponsor of, would further address this problem by setting up a reimbursement program to "rip and replace" vulnerable equipment from those networks. While we still have some details to work out on the way to markup, the program is modeled on the FCC's so-far-successful broadcast incentive repack reimbursement program. We need to get this right; it is critical to our national security but also our competitiveness as we start rolling out new technologies.

This brings me to another topic that I raised at 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 in this regard. 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. This past week, my staff saw this card posted to a bulletin board by the Rayburn cafeteria—details are pretty scant who is behind this campaign that just lists a litany of issues and why 5G is supposedly bad. It collects numerous stories around the country on things wrong with 5G—ironically one of the stories is about 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 risks from 5G, and that Cornell University research showed 5G networks to be safer than previous networks—So, we must be vigilant about efforts to influence our thinking in this space and I hope

the committee will look ahead at other efforts are being pursued to stifle our Internetarchitecture.

I look forward to hearing about the other bills put forward by our members today as other thoughtful approaches to these challenges.

Thank you again for holding this hearing today.

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; DEAN R. BRENNER, SENIOR VICE PRESIDENT, SPECTRUM STRATEGY AND 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. 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 play 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 have only increased the attack surface; 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 resources, 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 risk 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 manage-

ment 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:]

Bobbie Stempfley, Managing Director, CERT Division
Carnegie Mellon University Software Engineering Institute

Hearing on "Legislating to Secure America's Wireless Future"
Before the Subcommittee on Communications and Technology of the
United States House of Representatives Committee on Energy and Commerce

Introduction

Chairman Doyle and Ranking Member Latta, thank you for the opportunity to participate in this hearing on the supply chain risks of the telecommunications industry. I've been a public servant working in IT, focused on the application of information and technology to national security missions for 25 years. I am the Managing Director for the CERT Division of the Carnegie Mellon University Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC) sponsored by the Department of Defense (DoD). As a leader in cybersecurity, the CERT Division partners with government, industry, non-governmental organizations, and academia to improve the security and resilience of computer systems and networks.

Role of Telecommunication Companies in Security Today and in the Future

The telecommunications sector is a global system, made up of companies, suppliers, and users, that make communication possible. The infrastructure created by the telecoms touches all of us and allows the transmission of data, whether it is video through the airwaves or cables, audio through the phone or Internet, or voice through wires or wireless transmission.

Because the telecom industry is responsible for the flow of information, it is inextricably linked to how we work, play, and live. Communication plays a central role in the fundamental operations of a society—from business to government to families. Whether you need to contact the police, "Google" an address, call your child, or connect citizens to their government, the telecom industry makes it possible. But these connections also have vulnerabilities that create attack surfaces in connected hardware, firmware, or software that must be secured and monitored.

Furthermore, the explosion of edge devices, such as mobile phones, within the telecom infrastructure has only increased the attack surface and therefore the responsibility of the telecoms to protect their users. The role the telecoms play buffering risks from devices they do not control or purchase (such as your home router) makes it all the more important for them to ensure the security of those parts they do buy. Ultimately, the supply chain for the telecommunications industry is vital to achieve security at scale.

Supply Chain Security

What Is Supply Chain Security?

Since the 1990s, the rapid growth of the Internet and its burgeoning role in the transfer of data between telecoms have blurred and blended the boundary between telecom equipment and information technology (IT) hardware. This blending is now defined as information and communications technology (ICT), which emphasizes the role of unified communications and the integration of telecommunications (telephone lines and wireless signals) and computers—as well as the enterprise software, middleware, storage, and audiovisual systems—that allow users to access, store, transmit, and manipulate information.

In the past, when government or business invested in a piece of machinery, appliance, or service, it could more or less expect the item to function as advertised. Checks and balances (such as licenses, warranties, regulations, legal recourse, and supplier reputation) reasonably ensured against defects or service failures. Unfortunately, such controls seem increasingly inadequate when applied to global supply chains for the complex information and communications technology—and technology-based services—that underpin critical capabilities in the telecommunications industry. Concerns about supply chain risk management in ICT include the possibility that counterfeit or maliciously tainted hardware and software might be used by the acquiring organization to its detriment.[1]

All organizations, regardless of sector or mission, have dependencies on others. Organizations are profoundly linked to sources of goods and services not directly under their control, but without access to these critical items, the organizations would fail to achieve their missions. The common challenge now is having confidence in the security practices and processes of entities on which an organization relies when the relationship with those entities may be, at best, an arms-length agreement. Furthermore, we are now faced with a situation where the capabilities of today's software technology environment, the need to outsource, and the interaction between off-the-shelf and open source software products have far outpaced our ability to effectively monitor and manage the risk using traditional methods.[2] With the critical roles that software holds in our operational environments, the impact of fakes, frauds, and malicious activities could be devastating.

We know all organizations have dependencies, but we can no longer rely on formal legal contracts to ensure that suppliers mitigate risk. That approach is ineffective and fails to provide the mechanisms, flexibility, and repeatability needed to manage risks across the entire global supply chain. Effective collection and consumption of cyber threat intelligence requires a managed approach to these dependencies. The veracity of information must be examined and sources evaluated for trustworthiness. An ever-expanding supply chain means that external

---

[1] Haller, J. "Supply Chain and External Dependencies Risk Management." Software Engineering Institute, Carnegie Mellon University. January 2015.
[2] Alberts, C.; Haller, J.; Wallen, C.; & Woody, C. "Assessing DoD System Acquisition Supply Chain Risk Management." *CrossTalk* (May/June 2017): 4–8.

dependencies must be rigorously measured and strategically managed for an organization to remain resilient. Consequently, today's evolving landscape requires a comprehensive risk-based approach to managing the supply chain. Its complex nature requires an approach that is sensitive to the hardware, software, and services involved in providing the information and communication capabilities that we rely on. These include addressing:

- Manufacturing and integration supply chains: Responsible for conceptualizing, designing, building, and delivering systems and hardware.
- Service supply chain: Responsible for providing services to acquirers. In a defense context, these include services that vary as widely as data processing and hosting, logistics services, and support for administrative functions.
- Software supply chain: Responsible for producing the software that runs on vital systems.

What Happens Without Supply Chain Security?

Our ICT assets are under constant attack, yet thwarting the active attacker is not something most designers, engineers, developers, or project managers normally consider or have been trained to address. Moreover, most fail to acknowledge the dangers of integrating third-party supplies that may already contain malicious software or hardware. Consequently, no matter how secure you think your systems might be, if your suppliers are not secure, your systems are at risk. Failing to consider the security of your supply chain endangers the daily communications of millions of people, organizations, agencies, corporations, and communities.

Any variety of malicious actors who may have intentions to damage equipment and facilities, steal trade secrets or other sensitive corporate data, alter sensitive information, or cause disruption and devastation can target the telecom infrastructure either from the outside in an attack or from within as a supplier. Therefore, maintaining good supply chain security is paramount to the preservation of integrity and trust in the systems.

We must recognize the telecom infrastructure as the backbone of essential services that depend on connectivity, such as emergency response, utility, transportation, and financial services, among others. Furthermore, telecoms provide vital infrastructure for national security; from natural disaster recovery, to homeland security, to communication of crucial intelligence, to continued military superiority, telecommunications play a pivotal role.[3] The ramifications of an attack anywhere on the telecom infrastructure could spread well beyond the point of origin and have the potential to affect entire nations, businesses, and private citizens.

---

[3] National Research Council, Division on Engineering and Physical Sciences; Computer Science and Telecommunications Board; & Committee on Telecommunications Research and Development. *Reviewing U.S. Telecommunications Research*. National Academies Press. 2006.

Future Recommendations: How Should Telecoms Secure the Supply Chain?

These bills are a very good first step in supply chain security. As the appropriate entities begin to implement supply chain security, encouraging resilience as a criterion in every stage of development and supply of ICT 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 sharing information about ICT risks that arise through malice or negligence. Suppliers and acquirers need standardized means 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 that can cause subsequent harm.

Fundamentally, the outcomes and risk factors we are seeking to manage are simple, even if the methods to accomplish them are not. (1) Suppliers follow practices that reduce supply chain risks. (2) Products provided by suppliers are acceptably secure. (3) The methods of distribution and/or transmission of the product to the purchaser guard against tampering. And (4) the product or service is used and sustained with acceptable security.

The Acquisition Security Framework and the External Dependencies Management element of the Cyber Resilience Model developed and validated through research at the CERT Division demonstrate that the following practice areas are elements of a mature supply chain risk management effort: relationships, engineering, secure product operations and sustainment, and supply chain technology and infrastructure.

1. Relationships

Supply chain risks are not just managed through technical means; rather they rely on the establishment and sustainment of a relationship between the members of the supply chain. We have moved beyond the day when we were concerned mostly with the identification and integration of "black-box" parts to a concern with more integrated systems with similarly integrated supply chains and dependencies. The ability to maintain production schedules also requires this same relationship management. Through these efforts, companies in the telecommunications sector will receive more insight into the risks and benefits provided by the suppliers.

2. Engineering

Engineering comprises practices to build appropriate cybersecurity controls into systems, operational technologies, and components and minimize the chance of accidentally inserting vulnerabilities. Quality products and services are the result of effective engineering practices and sound test processes AND include distribution and release mechanisms that ensure the released products meet defined requirements, design, and security controls.

An element of this practice area includes understanding the entities within the supply chain. At a basic level this might be a bill of materials, a familiar concept in physical-world manufacturing, such as cars and aviation, which codifies all the ingredients of a product into a list. The bill of materials enables understanding about a product and provides the ability to track defects and changes through the supply chain. Such an inventory can be done with not only hardware components but also software and service components.

The National Telecommunications and Information Administration (NTIA) is over a year into a multistakeholder process for software bills of materials (SBOMs), nearing the end of Phase 1.[4] The CERT Division is co-chairing the Framing Working Group, which is developing and executing an approach for how manufacturers and vendors can communicate useful and actionable information about third-party software components and how enterprises can use this data to inform better security decisions and practices. The goal of this initiative is to foster a market that offers greater transparency to organizations, which can then integrate this data into their risk management approaches. The Framing Working Group has several whitepapers forthcoming.

SBOMs are already being used for license compliance, mainly when commercial vendors include open source components. Just as in the physical world, the supplier of the component, part, or software must define it and provide the SBOM. The NTIA process is examining existing formats, such as the software package data exchange (SPDX) and software identification (SWID) tags. The SBOM has to support nesting, recursion, and relationships (the physical world calls this the multi-level BOM). Lastly, telecom dependencies can be complex, and often key dependencies, like public services (e.g., law enforcement and shared infrastructure) can be overlooked without a proper accounting.

3. Secure Product Operations and Sustainment

Supply chain concerns do not end when the product or service reaches deployment. The telecoms and their suppliers must maintain products and services in their most secure configuration and with the most recent updates. This requires not only patching what the telecoms own, but also involving suppliers to ensure that any impacted fielded capabilities are also operating with the securest versions. This need demonstrates an important use case for the above-mentioned bills of materials, and specifically SBOMs. Telecommunications systems have multi-vendor vulnerabilities and no definitive knowledge about who or what is affected. SBOMs can provide this knowledge. It is not clear what else can.

4. Supply Chain Technology and Infrastructure

With the integration of development and supply chains, it is also important to focus on the efforts to secure the technology and infrastructure used to operate the supply chain itself. These efforts range from the need to secure the tools used to develop, integrate, and test software to the efforts to sustain situational awareness requirements for suppliers themselves.

---

[4] https://www.ntia.doc.gov/SoftwareTransparency

These practice areas cover the range of risk factors that have to be addressed as a part of a mature effort to manage the external dependencies and the supply chain.

Table 1. Mapping of Practice Areas to Risk Factors[5]

	Supplier Capability	Product Security	Product Distribution	Operational Product Control
1. Relationship Formation	x			
2. Relationship Management and Governance	x			
3. Engineering		x	x	
4. Secure Product Operation and Sustainment				x
5. Supply Chain Technology Infrastructure	x	x	x	x

Supply chains can be complex. Communication provider supply chains are often global and support software, hardware, and services that provide vital capabilities for public safety, national security, and general well-being. 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 vectors, and supplier security information should be shared along with mitigation plans whenever possible. One good way to collaboratively orchestrate industry and government response to these attacks is through the Common Vulnerabilities and Exposures (CVE) List. The CVE is an extensive listing of publicly known vulnerabilities found after ICT components have been deployed, and it has enabled our operations groups to prioritize, patch, and remediate nearly 60,000 openly reported vulnerabilities. Remediation is a crucial part of the security process, and while our work with the Defense Industrial Base (DIB) highlights the benefits of information sharing, it also emphasizes the need to ensure that everyone at the table, big or small, is able to take appropriate action to mitigate the threats.

Lastly, we should guard against the false choice between security and innovation. It is common to hear that regulations hinder or prevent innovation. Yet regulated industries, such as health care and finance, still practice innovation. Although it is difficult to predict the future impact of telecommunications technologies, services, and applications not yet invented, the technology

[5] Alberts et al., p. 7.

must continue to evolve quickly, and the industry must prevent security technology and concepts from becoming pacing factors in this evolution. Both innovation and security are necessary, and it is possible to have both.

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, and 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 4GLTE across five counties, including many areas where ours is the only signal present. Not only do our customers depend on our network, but on 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 deserves 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:]

Legislating to Secure America's Wireless Future

Testimony of John Nettles

President

Pine Belt Communications, Inc.

Before the

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Communications and Technology

September 27, 2019

Chairman Doyle, Ranking Member Latta, and Members of the Subcommittee, thank you for the opportunity to testify about how to secure communications networks while ensuring that wireless services are not cut off in rural America, a result that would be a step backwards on our nation's goal to close the digital divide.

I am John Nettles, the President and CEO of Pine Belt Communications. We are a family owned and operated company with deep roots in rural Alabama. My father established the landline arm of the company in late 1950's shortly after returning to his birthplace of Arlington to establish his medical practice. With no viable telephone system serving the area at that time, he realized that the place was behind times and could greatly benefit from modern telecom services. After a couple of years of trial and error, he launched commercial operations in 1958 filing the organizing documents on October 28th, just 22 days after I was born. Over the course of the following 60 years, we have worked hard to maintain our localized management and operating structure by keeping the company in the family.

We take pride in the economic contributions we are able to make to the communities we serve. We continue to work diligently to keep pace with the rapid advancements in technology and the intense capital requirements that characterize the industry. In doing so, the company has evolved into a state-of-the-art operation providing wired and wireless voice, video and data services to parts of the Alabama Black Belt.

We launched our wireless network in 1995 with three analog sites covering two counties. Today we operate 65 sites over which we provide 4G LTE services in five counties including many areas where ours is the only signal present. Our service footprint is mainly an agrarian area with the pine tree being the dominant crop, thus the name of our company, Pine Belt. The area is completely void of any Federal Interstate road mileage and has only a relatively small amount of four lane US Highways. The population density of our current service area is approximately one-fourth that of both Alabama and the

United States of America. Yet, modern, state-of-the-art coverage is without doubt just as important to the area we serve as it is those areas with above average population densities. This is evidenced by the reality that not only do our retail customers depend on our wireless services, but also by the fact that, on any given day, we will provide connectivity, including access to 9-1-1 emergency services, to as many 30,000 unique visitors, most of which are just passing through.

We have been able to remain relevant to the local telecom landscape, despite our rural footprint, by leveraging assets and private capital from debt markets and availing ourselves to the various federal grant, loan, and support programs when the opportunities presented themselves. And throughout the last 60 years, we have remained true to the mission my father adopted as the company was founded: to enhance the quality of life for our customers and partners by providing the highest quality of service at the best possible price.

To be clear, Pine Belt fully supports efforts to harden today's telecom networks for robust cybersecurity and to protect those networks from potential national security threats. Yet, while the industry buzzes with excitement of the great things that will soon come to bear as 5G networks are built-out, we at Pine Belt and numerous other small companies like us across the country have been all but frozen in our tracks since early last year by the cloud of uncertainty cast over us when the presence of certain vendor equipment in our networks was publicly called into question. In that respect, we greatly appreciate this Subcommittee's work to provide certainty to all carriers regarding what equipment can and cannot be used and, of equal importance, to provide desperately needed resources to allow carriers like Pine Belt to take the steps necessary to secure our networks. It is imperative that all carriers have access to equipment that is secure. And as in Pine Belt's case, when it is determined that equipment previously purchased with government assistance, for the purpose of meeting established public policy objectives using mandated lowest possible cost methodologies, must be removed and replaced for national security reasons due to certain vulnerabilities unknown at the time

of purchase, additional assistance is both in order and necessary, particularly for smaller and rural carriers that lack economies of scale. The Secure and Trusted Communications Networks Act and the Network Security Information Sharing Act take steps towards these goals.

How We Got Here

Pine Belt has significant interest in legislation before the Committee today, as well as proceedings before the Federal Communications Commission ("FCC") regarding supply chain security along with the Executive Order on Securing the Information and Communications Technology and Services Supply Chain issued by the President earlier this year. This is because our current wireless network was rebuilt in 2014 through 2017 with equipment from ZTE. Prior to our ZTE deployment we were operating a 2G network built with Lucent equipment originally installed in 1999. We relied on this equipment well past its manufacturer supported life keeping it in operation during a time in which there was little emphasis on making cost effective capital available to pure rural market operators such as us. Had it not been for the FCC's work to create the Mobility Fund Phase I ("MFI") program pursuant to the 2011 Universal Service and Intercarrier Compensation reform order, it is almost a certainty that we would have had to shutter our wireless business.

Through MFI, the FCC provided up to $300 million in one-time support for carriers to preserve and expand service where advanced mobile voice and data services were not available. Importantly, it was also the first mechanism to provide Universal Service Fund ("USF") Support through a reverse-auction in which winning auction bids were those that had the lowest cost to serve the greatest number of road-miles. Adopted in the spirit of carefully directing scarce USF resources, it is now clear that this mechanism led to some undesirable consequences in that several carriers deployed equipment that is now considered as presenting security risks. It is important to note that at the time, no vendor selections were prohibited in the auction process nor were additional resources available for the

deployment of any specific equipment. Our main performance criterion was to provide as much coverage possible as inexpensively as possible.

As part of Pine Belt's MFI experience, we solicited quotes from five different vendors. ZTE's bid was almost one-third of that of the highest bidder, and 25 percent below the second lowest bidder. With no restrictions in place and facing deployment challenges to serve our sparsely populated area, this equipment selection was a no-brainer. This selection not only enabled us to meet our mandated MFI buildout requirement, but also provided us with a reliable platform on which we could quickly deploy 4G LTE and VoLTE. And, despite the challenges of providing service across our low-density footprint, we were optimistic that this experience would allow us to provide the latest services to our community.

As the uncertainties became public regarding whether we would be able to continue to use deployed ZTE equipment, however, we also began to encounter delays in our routine expansion efforts. One such example comes from last year when we were wrapping up installation of a base station in a small town with a population of 26. As we approached project completion, we were significantly delayed in our ability to turn on LTE at the site due to uncertainty resulting from several Federal sanctions levied on ZTE for things of which we had no prior knowledge and absolutely zero involvement. Another more significant situation concerns our efforts to turn-up VoLTE service. That aspect of our 4G upgrades has essentially come to a complete stand still. A third and even larger example involves the numerous questions we have as to how we will put to use the 600 MHz spectrum we purchased in the FCC Auction 1002 and the millimeter wave licenses we purchased this year in Auction 101 given the fate of our network vendor. So, one could say, much like many other small carriers providing service in rural areas, absent steps from Congress and other Federal agencies, our network strategies are frozen at a time when they should instead be focused on expansion and upgrades to the next generation services. In many areas where Pine Belt provides service, because there is no other provider, this could mean the

loss of service entirely and potential squandering of $20 million plus in investments in modern wireless services for rural Alabama.

Legislation Before the Committee Is Necessary to Secure Rural Networks

While our experience regarding these issues in recent years has been one of uncertainty and concern, I am optimistic that working with Congress and other Federal agencies we can establish reasonable, sound policies and provide the essential financial resources needed to secure existing communications networks, allowing carriers to return to the work of meeting the exponentially growing demand for wireless services and laying the groundwork for the upgrades needed for rapid and timely deployment of 5G to all corners of the US, both urban and rural. The legislative efforts pending before this Subcommittee take significant steps to doing just that and plot a path to the future, by:

- Establishing the Secure and Trusted Communications Networks Reimbursement Program.

  As discussed above, Pine Belt has been able to provide wireless services to our community because of federal grant, subsidy, and loan programs, combined with our own internally generated financial resources. As the business case was challenging even before considering supply chain security issues, and initial network deployments were funded in part through support programs, the new reimbursement program is necessary to assist smaller carriers in replacing covered equipment in order to secure communications without reducing or eliminating coverage in rural areas.

  I applaud the Subcommittee for its work to establish the Secure and Trusted Communications Networks Reimbursement Program. With estimates to rip-and-replace covered network equipment as high as a billion dollars or more, financial analysts such as those at CoBank have noted that many rural operators will be unable to secure funding without government support.

The creation of this program is vital to support the national security policies we are discussing today without depriving rural America of the latest technology innovations.

- Determining a List of Covered Communications Equipment or Services.

  Smaller carriers serving rural areas require certainty to know what equipment and services can and cannot be deployed without creating risks to communications networks. Additional clarity provided by provisions of legislation before the Committee today will provide needed guidance while replacing covered equipment in the near future and beyond.

- Mitigating Burdens.

  As a small business, Pine Belt strongly supports legislative efforts to direct the FCC to take steps to mitigate administrative costs and burdens associated with participation in the Secure and Trusted Communications Networks Reimbursement Program.

- Targeting Network Risks.

  The legislation classifies covered equipment as that which is "capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles." Pine Belt supports consideration of all efforts to target network risks to eliminate the requirement for unnecessary replacement of network components that do not pose security risks, including radio access network components that are incapable of providing switching services or visibility into user data.

- Supporting Information Sharing.

  While nationwide service providers have resources and staff dedicated to information sharing with federal agencies on a day-to-day basis, smaller providers do not enjoy the same luxury of constant communication. Accordingly, I support the efforts through the Network Security Information Sharing Act to ensure that all carriers are provided the information they need to make decisions that support network security and trust in their communications networks.

Congressional Action is an Urgent Need

As Congress considers these critical national security issues, it is important to ensure that steps are taken in a timely manner to support national security. Efforts are currently underway, including through the Executive Order and pending proceedings before the FCC, to prohibit use of covered equipment. As FCC Commissioner Geoffrey Starks noted last week at the Competitive Carriers Association Annual Convention, "This is a national problem that deserves 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." Swift Congressional action is required to provide resources for replacement of covered equipment, which is particularly needed for carriers who are unable to cover the costs of replacement without financial assistance from the federal government.

With the implementation of the Executive Order looming, Federal policy may prohibit use of covered equipment without providing a way for Pine Belt to continue to provide service to its customers and other wireless users that travel through our service area. There is no time to waste in ensuring that necessary resources are available to remove covered communications equipment and to replace network gear that poses security risks with secure equipment and services, and continued action from Congress to further legislation considered today is needed to support this transition.

Other Bills Under Consideration Today Increase Certainty

In addition to today's consideration of legislation to secure wireless networks and share information to support that goal, the Subcommittee is also considering other bills that help wireless carriers take steps to confidently invest in existing and future technologies. Specifically, the idea that the Federal government may nationalize the wireless market threatens to upend billions of dollars invested in spectrum and network deployments from the private markets. While there is an appropriate role for regulation and oversight, the Federal government should not be in the business of

competing with the private sector. I appreciate the bipartisan efforts in the Eliminate From Regulators Opportunities to Nationalize The Internet in Every Respect Act, or the E-Frontier Act, to put that prohibition into statute.

Additionally, all carriers require access to sufficient spectrum resources to provide wireless services. That is true for nationwide wireless carriers serving millions of customers as well as smaller carriers serving rural markets. Like all carriers, Pine Belt pursues access to spectrum wherever possible, including participation and placing winning bids in spectrum auctions. It is also true that as a finite resource, policymakers must carefully consider how each spectrum band is allocated and used, including Federal use. I applaud the efforts to promote spectrum efficiency and coordination through the Studying How to Harness Airwave Resources Efficiently Act of 2019, or the SHARE Act, to support research and development around innovative technologies and techniques to facilitate sharing of spectrum, both between Federal entities and, where clearing and reallocation is not possible, with non-federal users. As technologies have evolved, so too should policies regarding spectrum allocations to support continued wireless growth. These and other efforts before the Subcommittee, including standards and strategy developments, all play important roles in securing communications networks.

This Committee has steadfastly worked to ensure that all Americans have access to the social, economic, educational, health, and public safety opportunities that rely on robust wireless services. I commend the steps the Committee has taken to support our wireless future. We at Pine Belt genuinely want to continue to be a part of the business landscape of our small corner of the country by providing the latest services to our neighbors, but we can only turn to our wireless future after removing the uncertainty regarding the equipment in place today and abiding by the many policies that shape our operating and investment environments. Thank you for your focus and leadership on these critical

issues, and I greatly appreciate the opportunity to share our story. I welcome any questions you may have.

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 are 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:]

Testimony of Harold Feld
Senior Vice President
Public Knowledge

Before the
U.S. House of Representatives
Committee on Energy & Commerce
Subcommittee on Communications & Technology

"Legislating to Secure America's Wireless Future"

Washington, DC
September 27, 2019

HEARING ON
"LEGISLATING TO SECURE AMERICA'S WIRELESS FUTURE"

Harold Feld, Senior Vice President
Public Knowledge

Chairman Doyle, Ranking Member Latta, thank you for inviting me to testify here today. Public Knowledge is pleased to endorse the SHARE Act. Investment in Federal spectrum sharing will have enormous advantages to the federal government and to commercial use of spectrum. Effective dynamic management will do more than free up federal spectrum for auction or open up new federal spectrum for unlicensed access. Technology developed as a result of the SHARE Act will enable federal users to dynamically access better quality spectrum on an as needed basis in a more efficient manner, creating a win for federal users. At the same time, study of the CBRS band will move us closer to the ability to accommodate a mix of priority federal users, licensed interference-protected commercial users, and unlicensed users in the same frequency bands – the Holy Grail of efficient spectrum use.

Public Knowledge is also pleased to support the "Promoting United States Leadership Act of 2019" (PUSLA). Public Knowledge believes strongly that participation by civil society in international standards bodies will dramatically improve the standards process for all. It will also help protect against the use of standards bodies for illegal collusion – an allegation that has emerged from time to time as a consequence of the closed nature of standards bodies. Public Knowledge also supports the Resolution by Mr. Flores on the Prague Protocols as common sense security recommendations for 5G networks.

Public Knowledge generally supports the concepts of the "Secure and Trusted Communications Act of 2019" (STCA) and the "Network Security Information Sharing Act of 2019" (NSISA). However, we recommend several changes to improve the STCA. STCA requires several modifications for due process purposes, such as a mechanism to challenge inclusion on the covered list and a mechanism to seek removal from the covered list. We also believe that reimbursement should not be limited to equipment purchased before August 2018 – especially if new providers are added to the covered list.

We take no position on the "Secure 5G and Beyond Act of 2019," in our testimony.

Finally, we oppose the E-FRONTIER Act as unnecessary and a potential source of negative unintended consequences. The Federal Government cannot build a new network without an appropriation from Congress. This provides more than adequate protection in the event that a future administration should ever seek to move beyond consideration of a national network. On the other hand, the federal government has numerous communications assets – such as spectrum and fiber – which may be of great value if made accessible to the public in emergencies or for rural broadband. The law as written would potentially prohibit any sort of public/private partnership, spectrum sharing agreement, or emergency provision of services. Given the ability of Congress to refuse to appropriate money for any unwanted federal activity, the more prudent course is to simply maintain the status quo.

I address details as to the SHARE Act, PUSLA, NSISA, STCA, and E-FRONTIERS below.

The SHARE Act of 2019 Would Create A Much-Needed Revolution In How Government Manages Spectrum To The Benefit of Federal Users As Well As Commercial users.

The SHARE Act would promote the development of new spectrum technology to allow federal agencies to share spectrum on a more dynamic basis. This would potentially revolutionize spectrum management for federal agencies. At present, federal agencies allocate spectrum in essentially the same way we have for decades, and the sad state of the Communications Act in this regard reflects our failure to acknowledge the march of technology. For example, Section 323 of the Communications Act requires that, in the event of interference between government users and commercial users, government users shall "transmit radio communications or signals only during the first 15 minutes of each hour."[1] While this was cutting edge 'time-division multiplexing' in 1927 when the statue was first written, we can surely do better today.

Dynamic sharing, once proven and reliable, would allow the federal government to move away from the existing allocation process that requires agencies to seek specific allocations of spectrum and invest in equipment limited to the specific frequencies allocated for the federal agency. This means that agencies may face spectrum constraints at critical times, while retaining unused spectrum allocations against future need. This problem is often further aggravated by the age and inefficiency of equipment. To make matters worse, each federal agency is responsible for its own equipment from its own budget. Rather than think of federal users as one giant user able to achieve economies of scale and match spectrum capacity needs with the specific mission, we currently atomize our spectrum policy across the federal government. This locks in historic allocations,

[1] 47 U.S.C. §323(b).

drives up overall equipment cost, and generally interferes with the ability to supply all branches of government with the reliable, cutting edge equipment needed to successfully complete operations in the digital age.

By creating a test bed for spectrum sharing among federal users – and by studying the CBRS system for accommodating federal priority users with commercial users – we can take the first step forward in modernizing federal spectrum management. It is extremely unfortunate, not to mention bad policy, to simply view enhanced federal sharing capacity as a means of clearing more spectrum for auction, or for finding ways to accommodate federal users and unlicensed users to co-exist. While it is inevitable that enhanced spectrum efficiency on the part of the government will provide such opportunities for expanded commercial use, the real value of the SHARE Act for the future will be technology that provides to all agencies access to more and better spectrum on an as needed basis while reducing the overall federal spectrum footprint.

Enhancing Federal Spectrum Sharing Will Improve National Security and Our Ability To Work With Allies on Humanitarian Missions.

As members of the Subcommittee are aware, the activation in Mexico of a new commercial cellular network has created significant interference issues with public safety licensees operating along the border.[2] This is a dramatic example of the problems faced by federal and commercial users with regard to frequency coordination with other countries. Although participation in the International Telecommunications Union (ITU) is

[2] *See* Vic Kolenc, "Mexico Cellular Network Is Problem for U.S. Phone Service, El Paso Emergency Responders," El Paso Times (September 20, 2019). Available at: https://www.elpasotimes.com/story/money/business/2019/09/20/mexico-cellular-network-disrupts-wireless-communications-united-states-mexico-border/2347529001/ (last visited September 24, 2019).

helpful for harmonizing global use, it does not prevent countries from adopting different band plans or different frequency allocations.

Developing ways to share spectrum without mutual interference will directly benefit federal users on the borders or when deployed abroad. Whether spectrum sharing techniques and technologies developed pursuant to the SHARE Act require mutual cooperation, or are simply "plug and play" by federal users to avoid interference, we can anticipate significant spin off benefits in addressing problems such as those currently plaguing emergency responders along the border with Mexico. These technologies will also provide ways for our military or other federal responders – such as aid personnel dispatched for disaster relief – to operate in coordination with host countries.

CBRS Represents A Major Breakthrough for Sharing Between Federal Users, Licensed Users and Unlicensed Users That Points The Way for Future Cooperation.

Changes to spectrum access assignment happen only slowly, and with great resistance. Formalizing the process of permitting unlicensed spectrum underlays took most of the 1980s, for example. Ultra-Wideband (UWB) took years, and is only just now potentially coming into wide adoption with Apple's decision to include an UWB chip in the iPhone 11.[3]

All of this makes the relatively rapid adoption and investment in Commercial Broadband Radio Service (CBRS) that much more remarkable. CBRS represents the first effort to develop a technology capable of accommodating federal users, exclusive commercial licensed users, and unlicensed users in the same general set of frequency

[3] *See* Jason Snell, "The U1 Chip In the iPhone 11 is the Beginning of an Ultra Wideband Revolution," Six Colors (September 13, 2019). Available at: https://sixcolors.com/post/2019/09/the-u1-chip-in-the-iphone-11-is-the-beginning-of-an-ultra-wideband-revolution/
(last visited September 24, 2019).

bands on a dynamic basis.[4] Although the FCC finalized rules for the band in 2015. The determination of the current FCC to conduct a new rulemaking and make substantive changes to the rules for allocating the Priority Access Licenses (PALs) created considerable, unnecessary delay. Nevertheless, the approval by the FCC last week of 5 spectrum access system (SAS) providers has now opened the door to a projected billion dollars in investment by 2023.[5]

The early success of CBRS – despite significant initial resistance and a two-year delay imposed by the current FCC – highlights the importance of studying it as a model for future spectrum sharing. In particular, CBRS has empowered users to access spectrum reserved for licensed users until the licensees actually activate their systems – a function called "use or share." For over a decade, wireless experts and rural advocates have explained that "use or share" technology holds great promise in bringing wireless broadband to rural areas neglected by licensees. As a general rule, licensees focus deployment in areas of greater population density, leaving communities with much sparser population densities with either subpar service or no service at all. Use or share allows small wireless ISPs (WISPs) or even individuals to deploy affordable, off-the-shelf technology in areas that licensees have no interest in serving. Nevertheless, incumbent licensees have strenuously resisted efforts to incorporate use or share into license rules.

---

[4] Technically, the "General Authorized Access" (GAA) is licensed by rule under 47 U.S.C. §307(e). As a practical matter, however, it functions for users in the same way as unlicensed access.

[5] Kendra Chamberlain, "CBRS RAN Market Investment to Surpass $1B by 2023: Dell'Oro Report," Fierce Wireless (March 22, 2019). Available at: https://www.fiercewireless.com/wireless/cbrs-ran-market-investments-to-surpass-1b-by-2023-dell-oro-report
(Last visited on September 24, 2019).

The CBRS deployment will prove the technical feasibility of use or share, and its value to both unserved communities and to licensees. In the event the licensee wishes to deploy in the area, the existing users will default back to the available GAA, so that no existing network will lose access. Crowded urban areas will provide valuable data on the usefulness and feasibility of use or share in areas where licensed deployment can be expected to be swift and intense, while rural areas will demonstrate the value of keeping spectrum in productive use despite the absence of licensee investment.

PUSLA Will Improve the International Standards Process And Promote Innovation, Competition and Consumer Protection.

Standards can fix policy just as easily as any rulemaking. The decisions that are made in standards bodies impact consumer protection concerns such as personal privacy. But often no one is present in these standard meetings to raise these concerns. In addition, because standards bodies bring together industry rivals, they may become avenues for collusion. As Adam Smith warned: "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public or a contrivance to raise prices."[6] On multiple occasions rumors have circulated that large incumbents have attempted to manipulate the standard setting process to the detriment of smaller competitors.[7] To be clear, we do not suggest that the standard setting process is generically suspect or a bad thing. To the contrary, industry standards developed through recognized standard-setting bodies play an important role in promoting competition and developing numerous improvements and innovations that benefit consumers. But even

[6] The Wealth of Nations, Book 1 Chapter X.
[7] *See, e.g.,* Cecilia Kang, "U.S. Investigating AT&T and Verizon Over Wireless Collusion Claims," New York Times (April 20, 2018). Available at: https://www.nytimes.com/2018/04/20/technology/att-verizon-investigate-esim.html (Last accessed September 24, 2019).

without concerns about possible anti-competitive or anti-consumer conduct, it is important for a wide range of stakeholders to be represented in the major international standard setting bodies to protect American interests and improve the quality of standard setting generally.

Additionally, involvement of civil society in ITU settings has proven important to advancing the national goals of the United States in defending Internet freedom and enhancing the general credibility of the United States delegation. I participated with the United States delegation to the World Conference on International Telecommunications (WCIT) in 2012, and can say from personal experience that the integration of civil society stakeholders and industry stakeholders enormously improved our ability to influence outcomes.

PUSLA offers an important first step in providing access to technical knowledge necessary to participate in international standard setting bodies. This could be improved by a more explicit commitment to civil society engagement, and by making funds available to cover dues and travel costs for representatives from civil society or small businesses. Even without these, however, Public Knowledge supports PUSLA and urges the Subcommittee and full Committee to move it forward.

The NSISA and STCA Underscore the Need To Acknowledge The Reality That Broadband and VOIP Are Title II Communications Services.

That Congress needs to pass special legislation to protect our critical communications infrastructure should highlight one thing clearly. Broadband is a Title II telecommunications service. Time and again, Congress finds itself reinventing provisions of the Communications Act using cumbersome circumlocutions to include voice over IP (VOIP) and broadband because the same logic that compelled inclusion of these concepts

in the Communications Act apply with equal force to the critical communications infrastructure of today. Just as the Communications Act makes the reliability and security of communications infrastructure central to the mission of the FCC, we find ourselves updating this concept for cybersecurity. Despite the insistence that broadband and VOIP networks are so radically different from "communications" that they should not be included in the same statutory framework, we find ourselves once again – as we did with universal service, pole attachments, and just about every other provision related to telecommunications networks – classing broadband and VOIP with other communications providers and applying the same necessary safeguards.

Congress should simply acknowledge this reality and restore broadband to Title II classification (and clarify that interconnected VOIP is also Title II). The House already took this step earlier this year. It is time for the Senate to pass the Save the Internet Act. Indeed, in a fine irony, the FCC Notice of Proposed Rulemaking referenced in STCA (proposing to prohibit USF recipients from purchasing equipment or services from covered entities) cites as its primary source of authority 47 U.S.C. §201(b).[8] If anything should highlight the obstinate folly of refusing to recognize the value of Title II classification and its relevance to broadband and VOIP, one would think that the current Commission's continued reliance on Title II generally and Section 201(b) specifically, to address broadband security vulnerabilities would be it.

NSISA's Information Sharing Regarding Communications Supply Chain Risks Is Useful for Shoring Up Key Vulnerabilities in Network Equipment and Devices.

[8] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, *Notice of Proposed Rulemaking* Docket No. 18-89 ¶35.

As cybersecurity expert Bruce Schneier warned just this week, every element of the supply chain is vulnerable – and the majority of attacks come from criminals not state-sponsored companies.[9] We have seen an explosion of ransomware against national and state governments. Security holes in devices have been exploited to bring down significant portions of the Internet. Exploitable weaknesses can come not only from the manufacturers or service providers under state control. As Schneier explains, open source programs can be manipulated by users, counterfeit chips can be introduced by bad actors, and patches to proprietary software can hide backdoors or other malware.

The NSISA provides a useful mechanism for communicating threats to our critical communications infrastructure gathered from foreign intelligence.

STCA Requires Modifications To Adequately Address Future Security Concerns, Ensure That Small Carriers That Act In Good Faith Are Held Harmless.

The STCA lacks important provisions to ensure due process. Because the STCA contains provisions for the FCC to add new companies, on an ongoing basis, the STCA should contain provisions by which an entity proposed for the updated list can challenge the designation before it goes into effect. Additionally, the STCA should require an explicit process for removal from the list. This should apply even to the named companies Section 2(b)(1)(A). We cannot predict today what our relationship will be with China in the future, nor can we predict what the relationship between these companies and the Chinese government will be in the future. But the statute provides no

[9] Bruce Schneier, "Every Part of the Supply Chain Can Be Attacked," New York Times (September 25, 2018). Available at: https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html?fbclid=IwAR1PneYnY2wD4AOHh83NiJyIM6ToSDLRhWEgL8SL21pX9u2T_y0Y7PEDwp4 (Last accessed September 25, 2019).

authority to remove any company, let alone the two companies specifically named in the statute.[10]

We do not believe that reimbursement should be limited solely to equipment purchased before August 14, 2018. It is unreasonable to presume that small providers constantly read the Federal Register and are aware of every FCC proceeding. This is particularly true for broadband providers, who have not generally been regulated by the current FCC. But even if providers are aware of the ongoing FCC proceeding, there was no reason to assume that the FCC would ultimately act on the proceeding. Furthermore, no provider potentially eligible for reimbursement could have foreseen that Congress would provide for reimbursement but punish providers who made the rational economic decision to keep buying low-priced equipment until the FCC told them to stop.

Finally, the statute as written would make it impossible for providers to receive reimbursement in the event the Commission identifies any future covered entities. The statute recognizes that new situations may come to light which would make it hazardous to buy equipment or services that may not even exist today. Under the statute, carriers will need to replace equipment from these newly identified threats. Given that the statute maintains the availability of funds for ten years, funds may be available to help these good faith purchasers ensure their networks comport with national security

[10] We note that specifically naming a company in the statute as subject to a specific penalty raises concerns that the statute will be considered an unlawful Bill of Attainder. Recent case law suggests that security measures such as this against companies that are at least partially owned or controlled by a foreign power may not constitute a Bill of Attainder but a reasonable security measure. *See Kapersky Lab, Inc. v. DHS*, 311 F. Supp. 3d 187 (D.D.C. 2018). Because this lies outside the scope of our expertise, Public Knowledge expresses no opinion on the matter.

determinations. It makes no sense to prohibit future injured parties from applying for reimbursement for expenses they could not predict would be problematic.

Securing our nation's critical infrastructure is our common responsibility. We should not ask small providers that are dependent on federal grants to provide service to rural America to bear the cost. Any provider that purchased equipment of services in good faith should be eligible to receive funding to replace listed equipment.

E-FRONTIER Is Unnecessary And Will Have Negative Unintended Consequences.

The E-FRONTIER Act, and its companion bill in the Senate, appear to be a direct response to press reports about an early-2018 recommendation within the Trump Administration to build a nation-wide, federal 5G network. This proposal has been roundly repudiated by the Trump Administration – most notably at a public event on 5G networks where he shared the podium with FCC Chairman Ajit Pai.[11] The FCC's Democratic Commissioners have likewise dismissed the proposed national network as misguided.[12] Nor could any Administration, now or in the future, build such a network without an appropriation from Congress. Like the hypothetical network the statute would prohibit, the E-Frontier Act is a solution in search of a problem.

Unfortunately, passing legislation is not merely a symbolic act. It has real, unintended consequences. The federal government provides numerous loans and grant programs. Without a review, it is likely that the E-FRONTIER Act will create needless

---

[11] Aaron Pressman, "Forget Rural Internet – This Was the Real Agenda at Trump's 5G Wireless Event," Fortune (April 12, 2019). Available at: https://fortune.com/2019/04/12/trump-ajit-pai-5g-wireless-auction-rural-internet/ (Last accessed September 25, 2019).

[12] Harper Neidig, "FCC Chair Opposes Nationalizing 5G Network," The Hill (January 29, 2018). Available at: https://thehill.com/policy/technology/371184-fcc-chair-comes-out-against-nationalizing-5g-network (Last accessed September 25, 2019).

confusion. For example, if the Department of Housing and Urban Development funds broadband in federal housing, would such a program violate the E-Frontier Act? Would operation of a network designed to bring service to rural hospitals, or to military housing outside a military base, constitute a "wholesale" or "retail" network? How will E-FRONTIER impact RUS recipients? Given the sweeping language of the E-FRONTIER Act, the enormous number of potential federal grants, and the increasing centrality of broadband in everything from housing to healthcare, the likelihood of some undesired negative consequence, such as discouraging valuable projects or encouraging grant challenges, seems almost certain.

Even worse, the E-FRONTIER Act will potentially curtail efforts to use federal assets such as spectrum or fiber to assist in natural disasters or provide broadband to rural areas. Consider the following examples. A massive hurricane sweeps away commercial networks, but federal fiber remains usable. The federal government wants to make the capacity available for wholesale use by carriers until they can restore their own service. The plain language of the E-FRONTIER Act would prevent any such helpful use of federal fiber or other communications assets. Or imagine if a military installation or federal research facility pulls fiber into an isolated rural community. Would we really want to prohibit any creative way in which the community might leverage federal fiber to close the local digital divide? Or imagine a federal agency contracts with a company to use federal spectrum, allowing the company to provide commercial service over any excess capacity. Would this constitute a federal wholesale or retail network under the sweeping language of the E-FRONTIER Act.

No one of these possibilities is particularly likely in the near term, but the likelihood that the E-FRONTIER Act will unintentionally diminish flexibility in federal projects, federal contracting, or federal disaster response is very real. Even if the risk seems remote, why take any risk at all? No federal network is planned, nor can any proceed without federal funding. If such a network ever did seem like a substantial possibility, Congress could pass targeted legislation then.

CONCLUSION

No one can argue that Congress should ignore the threats to our critical infrastructure or the importance of maintaining U.S. leadership in wireless technology. As discussed above, the SHARE Act and PUSLA are important investments in our wireless future. NSISA and STCA address critical network security needs, but should be modified as discussed above. The E-FRONTIER Act, however, is both unnecessary and creates unintended consequences.

Thank you and I am prepared to answer any questions at this time.

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 one 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 six 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, enable cars to communicate with other cars and infrastructure with much greater range and reliability than 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 allows 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 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:]

Before the

United States House of Representatives

Subcommittee on Communications & Technology

Hearing on

"Legislating to Secure America's Wireless Future"

Testimony of

Dean R. Brenner

Senior Vice President, Spectrum Strategy & Tech Policy

Qualcomm Incorporated

September 27, 2019

Chairman Doyle, Ranking Member Latta, and Members of the Subcommittee, my name is Dean Brenner, and I'm here today on behalf of Qualcomm, which was founded in a San Diego living room, but is now the world's leading 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 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; and, licensed, unlicensed, and shared—is essential for the rapid, broad 5G roll-out. We're 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 is now launched on four continents. More than thirty 5G networks, including those of all four US national operators, have launched and are expanding. Over twenty 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, hotspots, and fixed wireless devices. Our chips support both sub-7 GHz and millimeter wave bands, and the US was the first country to launch 5G in both sub-7 GHz 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 accelerate the 5G rollout:

- Dynamic Spectrum Sharing (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 ten 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 one 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 used for ultra-low latency, ultra-reliable 5G in factories, warehouses, and other venues. This

technology, along with new forms of Wi-Fi that Qualcomm is working on, would be deployed in new 6 GHz unlicensed spectrum now under consideration by the FCC.

- Qualcomm's 5G small cell chips will expand 5G to more people and locations, particularly indoors using millimeter wave spectrum.
- Last, cellular vehicle to everything (C-V2X) technology, first with 4G and then 5G, enables cars to communicate with other cars and infrastructure with much greater range and reliability than is possible with older DSRC technology. For C-V2X to be deployed, the FCC must waive or change the rules for 5.9 GHz spectrum, 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 Communications Security, Reliability & Operability Council.

Most recently, we appreciated the bipartisan May 9th letter sent from the Chairmen 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 Risk in Emerging 5G Implementations. The members of this CSRIC 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 multi-stakeholder group.

Finally, Qualcomm has been working on spectrum sharing for many years. We have worked directly with NTIA, the Defense Department, 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, gathering technical input from the government players, working with industry, leading joint public-private technical work, and speaking for the Executive Branch with a unified voice to make progress toward greater sharing. This process culminated most recently in the initial commercial deployments which have begun in the 3.5 GHz CBRS band—a great

development which increases the amount of mid-band spectrum for 4G and 5G. We're very pleased with the heightened interest across the federal government in sharing spectrum with industry, and we look forward to continuing to work through this process to enable more intensive spectrum sharing.

Thank you, and I look forward to answering your questions.

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. Yes. 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, and 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. Yes. 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 is 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. 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. These 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 backward.

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 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; 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 on 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. 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 equip-

ment 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 build out 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 then 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 used Mobility

Fund-1 money to build a 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 its 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, seven 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 was overseeing it, yes. 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 are 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.

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 integrated 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. Is there any—and anybody who 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 testbed? 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. OK. 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. OK.

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. OK.

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 appears at the conclusion of the hearing.]

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 ten 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.]

[Material submitted for inclusion in the record follows:]

PREPARED STATEMENT OF HON. ADAM KINZINGER

I thank my friend, Mr. Latta, for yielding.

The security of American communications and information networks is paramount to national security-a field I know fairly well from my time in the military, but this sword cuts both ways.

As we have seen through the years, certain foreign adversaries have systematically coerced their equipment manufacturers to embed backdoors 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 backdoors to launch cyberattacks or disrupt our communications.

In an effort to help the private sector avoid purchasing or installing this dangerous equipment, I worked with the Chairman, Mr. 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 the discussion today and I yield back to my friend.

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. RES. 575

Expressing the sense of the House of Representatives that all stakeholders in the deployment of 5G communications infrastructure should carefully consider and adhere to the recommendations of "The Prague Proposals".

IN THE HOUSE OF REPRESENTATIVES

Mr. FLORES submitted the following resolution; which was referred to the Committee on _____

RESOLUTION

Expressing the sense of the House of Representatives that all stakeholders in the deployment of 5G communications infrastructure should carefully consider and adhere to the recommendations of "The Prague Proposals".

Whereas 5G, the next generation (5th generation) in wireless technology, promises the next evolution of communications and information technology services, applications, and capabilities across every sector of business, government, entertainment, and communications;

Whereas the United States, Europe, China, and others are racing toward 5G adoption and upgrading existing networks, which will drive subsequent advances in artificial

intelligence, machine learning, smart homes, smart cities, robotics, autonomous vehicles, and quantum computers;

Whereas 5G will make possible the automatization of everyday activities and the use of the full potential of the Internet of Things;

Whereas these developments, while evolutionary, could include risks to important public interests, including privacy, data security, public safety, and national security;

Whereas in a highly connected world, disruption of the integrity, confidentiality, or availability of communications or even the disruption of the communications service itself can seriously hamper everyday life, societal functions, the economy, and national security;

Whereas the security of 5G networks is crucial for national security, economic security, and other United States national interests and global stability;

Whereas operators of communications infrastructure depend on a complex supply chain of technology from a global market of suppliers and service providers;

Whereas government security officials and experts from 32 countries came together in Prague in May of 2019 to work out guidelines for the deployment and security of 5G networks;

Whereas representatives agreed that "[m]ajor security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. These risks should be considered as part of the risk assessment based on relevant information and should seek to prevent proliferation of compromised devices and the use of malicious code and functions."; and

Whereas the Prague 5G Security Conference adopted security recommendations, which have come to be known as ''The Prague Proposals'': Now, therefore, be it

Resolved,

SECTION 1. SENSE OF THE HOUSE OF REPRESENTATIVES.

The House of Representatives—

(1) urges all stakeholders in the deployment of 5G communications infrastructure to carefully consider adherence to the recommendations of ''The Prague Principles'' (as described in section 2) as they procure products and services across their supply chain; and

(2) encourages the President and Federal agencies to promote global trade and security policies that are consistent with ''The Prague Proposals'' and urge our allies to embrace the recommendations of ''The Prague Proposals'' for their public 5G infrastructure.

SEC. 2. PRAGUE PROPOSALS.

The text of ''The Prague Proposals'' is as follows:

(1) ''POLICY''.—

(A) ''Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best

practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted.".

(B) "Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse.".

(C) "Laws and policies governing networks and connectivity services should be guided by the principles of transparency and equitability, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law.".

(D) "The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on

cybersecurity, the fight against cybercrime, or data protection.''.

(2) ''TECHNOLOGY''.—

(A) ''Stakeholders should regularly conduct vulnerability assessments and risk mitigation within all components and network systems, prior to product release and during system operation, and promote a culture of find/fix/patch to mitigate identified vulnerabilities and rapidly deploy fixes or patches.''.

(B) ''Risk assessments of supplier's products should take into account all relevant factors, including applicable legal environment and other aspects of supplier's ecosystem, as these factors may be relevant to stakeholders' efforts to maintain the highest possible level of cyber security.''.

(C) ''When building up resilience and security, it should be taken into consideration that malicious cyber activities do not always require the exploitation of a technical vulnerability, e.g. in the event of insider attack.''.

(D) ''In order to increase the benefits of global communication, States should adopt poli-

cies to enable efficient and secure network data flows.".

(E) "Stakeholders should take into consideration technological changes accompanying 5G networks roll out, e.g. use of edge computing and software defined network/network function virtualization, and its impact on overall security of communication channels.".

(F) "Customer—whether the government, operator, or manufacturer—must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and services.".

(3) "ECONOMY".—

(A) "A diverse and vibrant communications equipment market and supply chain are essential for security and economic resilience.".

(B) "Robust investment in research and development benefits the global economy and technological advancement and is a way to potentially increase diversity of technological solu-

tions with positive effects on security of communication networks.".

(C) "Communication networks and network services should be financed openly and transparently using standard best practices in procurement, investment, and contracting.".

(D) "State-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles, while taking into account trade obligations.".

(E) "Effective oversight on key financial and investment instruments influencing telecommunication network development is critical.".

(F) "Communication networks and network service providers should have transparent ownership, partnerships, and corporate governance structures.".

(4) "SECURITY, PRIVACY, AND RESILIENCE".—

(A) "All stakeholders including industry should work together to promote security and

resilience of national critical infrastructure networks, systems, and connected devices.".

(B) "Sharing experience and best practices, including assistance, as appropriate, with mitigation, investigation, response, and recovery from network attacks, compromises, or disruptions should be promoted.".

(C) "Security and risk assessments of vendors and network technologies should take into account rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services to deal with the rising challenges.".

(D) "Risk management framework in a manner that respects data protection principles to ensure privacy of citizens using network equipment and services should be implemented.".

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. 4459

To prohibit Federal funds from being used to purchase communications equipment or services posing national security risks, to provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. PALLONE (for himself, Mr. WALDEN, Ms. MATSUI, and Mr. GUTHRIE) introduced the following bill; which was referred to the Committee on

---

A BILL

To prohibit Federal funds from being used to purchase communications equipment or services posing national security risks, to provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Secure and Trusted Communications Networks Act of 2019".

SEC. 2. DETERMINATION OF COMMUNICATIONS EQUIPMENT OR SERVICES POSING NATIONAL SECURITY RISKS.

(a) PUBLICATION OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES LIST.—Not later than 1 year after the date of the enactment of this Act, the Commission shall publish on its website a list of covered communications equipment or services.

(b) DETERMINATION BY COMMISSION.—The Commission shall place on the list published under subsection (a) any communications equipment or service, if and only if the Commission determines that such equipment or service—

(1) is produced or provided by—

(A) Huawei Technologies Co. Limited, Zhongxing Telecommunications Equipment Corporation, or any subsidiary or affiliate of either such entity;

(B) any successor to any entity described in subparagraph (A); or

(C) any other entity, if the Commission determines, based exclusively on the determinations described in paragraphs (1) through (4)

of subsection (c), that such equipment or service produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons; and

(2) is capable of—

(A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; or

(B) causing the network of a provider of advanced communications service to be disrupted remotely.

(c) RELIANCE ON CERTAIN OTHER DETERMINATIONS.—In making a determination under subsection (b)(1)(C), the Commission shall rely solely on one or more of the following determinations:

(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.

(2) A specific determination made by the Bureau of Industry and Security of the Department of Commerce to place an entity on the entity list main-

tained by the Bureau and set forth in Supplement No. 4 to part 744 of the Export Administration Regulations (subchapter C of chapter VII of title 15, Code of Federal Regulations).

(3) A specific determination made pursuant to Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain), including any determination made by the Department of Commerce pursuant to regulations promulgated to implement such Executive Order.

(4) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 1918).

(d) UPDATING OF LIST.—The Commission shall periodically update the list published under subsection (a), as necessary to protect national security and to address changes in the determinations described in paragraphs (1) through (4) of subsection (c). For each 12-month period during which the list is not updated, the Commission shall notify the public that no updates were necessary during

such period to protect national security or to address changes in such determinations.

SEC. 3. PROHIBITION ON USE OF FEDERAL FUNDS.

(a) IN GENERAL.—

(1) PROHIBITION.—Federal funds may not be used to purchase, rent, lease, or otherwise obtain any covered communications equipment or service or to maintain any covered communications equipment or service previously purchased, rented, leased, or otherwise obtained.

(2) TIMING.—Paragraph (1) shall apply with respect to any covered communications equipment or service beginning on the date that is 60 days after the date on which the Commission places such equipment or service on the list required by section 2(a). In the case of any covered communications equipment or service that is on the initial list published under such section, such equipment or service shall be treated as being placed on the list on the date on which such list is published.

(b) COMPLETION OF PROCEEDING.—Not later than 90 days after the date of the enactment of this Act, the Commission shall adopt a Report and Order in the matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs

(WC Docket No. 18–89) that implements subsection (a), to the extent such subsection applies to a program administered by the Commission.

(c) APPLICATION TO OTHER AGENCIES.—Not later than 180 days after the date of the enactment of this Act, the head of each Federal agency that administers a program through which Federal funds are made available shall update the regulations for the program to comply with subsection (a).

SEC. 4. SECURE AND TRUSTED COMMUNICATIONS NETWORKS REIMBURSEMENT PROGRAM.

(a) IN GENERAL.—The Commission shall establish a reimbursement program, to be known as the ''Secure and Trusted Communications Networks Reimbursement Program'', to make reimbursements to providers of advanced communications service to replace covered communications equipment or services.

(b) ELIGIBILITY.—The Commission may not make a reimbursement under the Program to a provider of advanced communications service unless the provider—

(1) has 2,000,000 or fewer customers; and

(2) makes all of the certifications required by subsection (d)(5).

(c) USE OF FUNDS.—

(1) IN GENERAL.—A recipient of a reimbursement under the Program shall use reimbursement funds solely for the purposes of—

(A) permanently removing covered communications equipment or services purchased, rented, leased, or otherwise obtained before August 14, 2018, and replacing such equipment or services with communications equipment or services that are not covered communications equipment or services; and

(B) disposing of the equipment or services removed as described in subparagraph (A) in accordance with the requirements under subsection (d)(8).

(2) LIMITATIONS.—A recipient of a reimbursement under the Program may not use reimbursement funds to—

(A) remove, replace, or dispose of any covered communications equipment or service purchased, rented, leased, or otherwise obtained on or after August 14, 2018;

(B) purchase, rent, lease, or otherwise obtain any covered communications equipment or service, using reimbursement funds or any

other funds (including funds derived from private sources); or

(C) make network upgrades that go beyond the replacement of covered communications equipment or services, as determined by the Commission.

(d) IMPLEMENTATION.—

(1) REGULATIONS.—Not later than 270 days after the date of the enactment of this Act, the Commission shall promulgate regulations to implement the Program.

(2) SUGGESTED REPLACEMENTS.—

(A) DEVELOPMENT OF LIST.—The Commission shall develop a list of suggested replacements of both physical and virtual communications equipment, application and management software, and services.

(B) NEUTRALITY.—The list developed under subparagraph (A) shall be technology neutral and may not advantage the use of reimbursement funds for capital expenditures over operational expenditures, to the extent that the Commission determines that communications services can serve as an adequate substitute for the installation of communications equipment.

(3) APPLICATION PROCESS.—

(A) IN GENERAL.—The Commission shall develop an application process and related forms and materials for the Program.

(B) COST ESTIMATE.—

(i) INITIAL ESTIMATE.—The Commission shall require an applicant to provide an initial reimbursement cost estimate at the time of application, with supporting materials substantiating the costs.

(ii) UPDATES.—During and after the application review process, the Commission may require an applicant to—

(I) update the initial reimbursement cost estimate submitted under clause (i); and

(II) submit additional supporting materials substantiating an updated cost estimate submitted under subclause (I).

(C) MITIGATION OF BURDEN.—In developing the application process under this paragraph, the Commission shall take reasonable steps to mitigate the administrative burdens and costs associated with the application proc-

ess, while taking into account the need to avoid waste, fraud, and abuse in the Program.

(4) APPLICATION REVIEW PROCESS.—

(A) DEADLINE.—

(i) IN GENERAL.—Except as provided in clause (ii) and subparagraph (B), the Commission shall approve or deny an application for a reimbursement under the Program not later than 90 days after the date of the submission of the application.

(ii) ADDITIONAL TIME NEEDED BY COMMISSION.—If the Commission determines that, because an excessive number of applications have been filed at one time, the Commission needs additional time for employees of the Commission to process the applications, the Commission may extend the deadline described in clause (i) for not more than 45 days.

(B) OPPORTUNITY FOR APPLICANT TO CURE DEFICIENCY.—If the Commission determines that an application is materially deficient (including by lacking an adequate cost estimate or adequate supporting materials), the Commission shall provide the applicant a 15-day period

to cure the defect before denying the application. If such period would extend beyond the deadline under subparagraph (A) for approving or denying the application, such deadline shall be extended through the end of such period.

(C) EFFECT OF DENIAL.—Denial of an application for a reimbursement under the Program shall not preclude the applicant from resubmitting the application or submitting a new application for a reimbursement under the Program at a later date.

(5) CERTIFICATIONS.—An applicant for a reimbursement under the Program shall, in the application of such applicant, certify to the Commission that—

(A) beginning on the date of the submission of the application, the applicant will not purchase, rent, lease, or otherwise obtain covered communications equipment or services, using reimbursement funds or any other funds (including funds derived from private sources); and

(B) as of the date of the submission of the application, the applicant—

(i) has developed a plan for—

(I) the permanent removal and replacement of any covered communications equipment or services that are in the communications network of the applicant as of such date; and

(II) the disposal of the equipment or services removed as described in subclause (I) in accordance with the requirements under paragraph (8);

(ii) has developed a specific timeline (subject to paragraph (7)) for the permanent removal, replacement, and disposal of the covered communications equipment or services identified under clause (i), which timeline shall be submitted to the Commission as part of the application;

(iii) has taken, or will immediately take, all necessary steps to mitigate the security threat the covered communications equipment or services identified under clause (i) could pose to the network of the applicant until the equipment or services can be permanently removed and replaced

in accordance with the timeline described in clause (ii); and

(iv) in developing and tailoring the risk management practices of such applicant, will consult and consider the standards, guidelines, and best practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology.

(6) DISTRIBUTION OF REIMBURSEMENT FUNDS.—

(A) IN GENERAL.—The Commission shall make reasonable efforts to ensure that reimbursement funds are distributed as equitably as possible among all applicants for reimbursements under the Program according to the needs of the applicants, as identified by the applications of the applicants.

(B) NOTIFICATION.—If, at any time during the implementation of the Program, the Commission determines that the funds made available to the Commission to carry out the Program will not be sufficient to fully fund all approved applications for reimbursements under

the Program, the Commission shall immediately notify—

(i) the Committee on Energy and Commerce and the Committee on Appropriations of the House of Representatives; and

(ii) the Committee on Commerce, Science, and Transportation and the Committee on Appropriations of the Senate.

(7) REMOVAL, REPLACEMENT, AND DISPOSAL TERM.—

(A) DEADLINE.—The permanent removal, replacement, and disposal of any covered communications equipment or services identified under paragraph (5)(B)(i) shall be completed not later than 1 year after the date on which the Commission approves the application.

(B) GENERAL EXTENSION.—The Commission may grant an extension of the deadline described in subparagraph (A) for 6 months to all recipients of reimbursements under the Program if the Commission—

(i) finds that the supply of replacement communications equipment or services needed by the recipients to achieve the

purposes of the Program is inadequate to meet the needs of the recipients; and

(ii) provides notice and a detailed justification for granting the extension to—

(I) the Committee on Energy and Commerce of the House of Representatives; and

(II) the Committee on Commerce, Science, and Transportation of the Senate.

(C) INDIVIDUAL EXTENSION.—

(i) PETITION.—A recipient of a reimbursement under the Program may petition the Commission for an extension for such recipient of the deadline described in subparagraph (A) or, if the Commission has granted an extension of such deadline under subparagraph (B), such deadline as so extended.

(ii) GRANT.—The Commission may grant a petition filed under clause (i) by extending, for the recipient that filed the petition, the deadline described in subparagraph (A) or, if the Commission has granted an extension of such deadline under

subparagraph (B), such deadline as so extended, for a period of not more than 6 months if the Commission finds that, due to no fault of such recipient, such recipient is unable to complete the permanent removal, replacement, and disposal described in subparagraph (A).

(8) DISPOSAL OF COVERED COMMUNICATIONS EQUIPMENT OR SERVICES.—The Commission shall include in the regulations promulgated under paragraph (1) requirements for the disposal by a recipient of a reimbursement under the Program of covered communications equipment or services identified under paragraph (5)(B)(i) and removed from the network of the recipient in order to prevent such equipment or services from being used in the networks of providers of advanced communications service.

(9) STATUS UPDATES.—

(A) IN GENERAL.—Not less frequently than once every 90 days beginning on the date on which the Commission approves an application for a reimbursement under the Program, the recipient of the reimbursement shall submit to the Commission a status update on the work

of the recipient to permanently remove, replace, and dispose of the covered communications equipment or services identified under paragraph (5)(B)(i).

(B) PUBLIC POSTING.—The Commission shall make public on the website of the Commission each status update submitted under subparagraph (A).

(C) REPORTS TO CONGRESS.—Not less frequently than once every 180 days beginning on the date on which the Commission first makes funds available to a recipient of a reimbursement under the Program, the Commission shall prepare and submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on—

(i) the implementation of the Program by the Commission; and

(ii) the work by recipients of reimbursements under the Program to permanently remove, replace, and dispose of covered communications equipment or services identified under paragraph (5)(B)(i).

(e) MEASURES TO AVOID WASTE, FRAUD, AND ABUSE.—

(1) IN GENERAL.—The Commission shall take all necessary steps to avoid waste, fraud, and abuse with respect to the Program.

(2) SPENDING REPORTS.—The Commission shall require recipients of reimbursements under the Program to submit to the Commission on a regular basis reports regarding how reimbursement funds have been spent, including detailed accounting of the covered communications equipment or services permanently removed and disposed of, and the replacement equipment or services purchased, rented, leased, or otherwise obtained, using reimbursement funds.

(3) AUDITS, REVIEWS, AND FIELD INVESTIGATIONS.—The Commission shall conduct—

(A) regular audits and reviews of reimbursements under the Program to confirm that recipients of such reimbursements are complying with this Act; and

(B) random field investigations to ensure that recipients of reimbursements under the Program are performing the work such recipients are required to perform under the commit-

ments made in the applications of such recipients for reimbursements under the Program, including the permanent removal, replacement, and disposal of the covered communications equipment or services identified under subsection (d)(5)(B)(i).

(4) FINAL CERTIFICATION.—

(A) IN GENERAL.—The Commission shall require a recipient of a reimbursement under the Program to submit to the Commission, in a form and at an appropriate time to be determined by the Commission, a certification stating that the recipient—

(i) has fully complied with (or is in the process of complying with) all terms and conditions of the Program;

(ii) has fully complied with (or is in the process of complying with) the commitments made in the application of the recipient for the reimbursement;

(iii) has permanently removed from the communications network of the recipient, replaced, and disposed of (or is in the process of permanently removing, replacing, and disposing of) all covered commu-

nications equipment or services that were in the network of the recipient as of the date of the submission of the application of the recipient for the reimbursement; and

(iv) has fully complied with (or is in the process of complying with) the timeline submitted by the recipient under subparagraph (B)(ii) of paragraph (5) of subsection (d) and the other requirements of such paragraph.

(B) UPDATED CERTIFICATION.—If, at the time when a recipient of a reimbursement under the Program submits a certification under subparagraph (A), the recipient has not fully complied as described in clause (i), (ii), or (iv) of such subparagraph or has not completed the permanent removal, replacement, and disposal described in clause (iii) of such subparagraph, the Commission shall require the recipient to file an updated certification when the recipient has fully complied as described in such clause (i), (ii), or (iv) or completed such permanent removal, replacement, and disposal.

(f) RULE OF CONSTRUCTION REGARDING TIMING OF REIMBURSEMENT.—Nothing in this section shall be con-

strued to prohibit the Commission from making a reimbursement under the Program to a provider of advanced communications service before the provider incurs the cost of the permanent removal, replacement, and disposal of the covered communications equipment or service for which the application of the provider has been approved under this section.

(g) EDUCATION EFFORTS.—The Commission shall engage in education efforts with providers of advanced communications service to—

(1) encourage such providers to participate in the Program; and

(2) assist such providers in submitting applications for the Program.

(h) SEPARATE FROM FEDERAL UNIVERSAL SERVICE PROGRAMS.—The Program shall be separate from any Federal universal service program established under section 254 of the Communications Act of 1934 (47 U.S.C. 254).

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Commission $1,000,000,000 for fiscal year 2020 to carry out the Program. Such amount is authorized to remain available through fiscal year 2029.

SEC. 5. HOLD HARMLESS.

In the case of a person who is a winner of the Connect America Fund Phase II auction, has not yet been authorized to receive Connect America Fund Phase II support, and demonstrates an inability to reasonably meet the build-out and service obligations of such person under Connect America Fund Phase II without using equipment or services prohibited under this Act, such person may withdraw the application of such person for Connect America Fund Phase II support without being found in default or subject to forfeiture.

SEC. 6. ENFORCEMENT.

(a) VIOLATIONS.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of the Communications Act of 1934 (47 U.S.C. 151 et seq.) or a regulation promulgated under such Act, respectively. The Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Communications Act of 1934 were incorporated into and made a part of this Act.

(b) ADDITIONAL PENALTIES.—

(1) IN GENERAL.—Except as provided in paragraph (2), in addition to penalties under the Communications Act of 1934, a recipient of a reimburse-

ment under the Program found to have violated section 4, the regulations promulgated under such section, or the commitments made by the recipient in the application for the reimbursement—

(A) shall repay to the Commission all reimbursement funds provided to the recipient under the Program;

(B) shall be barred from further participation in the Program;

(C) shall be referred to all appropriate law enforcement agencies or officials for further action under applicable criminal and civil laws; and

(D) may be barred by the Commission from participation in other programs of the Commission, including the Federal universal service support programs established under section 254 of the Communications Act of 1934 (47 U.S.C. 254).

(2) NOTICE AND OPPORTUNITY TO CURE.—The penalties described in paragraph (1) shall not apply to a recipient of a reimbursement under the Program unless—

(A) the Commission provides the recipient with notice of the violation; and

(B) the recipient fails to cure the violation within 180 days after the Commission provides such notice.

(c) RECOVERY OF FUNDS.—The Commission shall immediately take action to recover all reimbursement funds awarded to a recipient of a reimbursement under the Program in any case in which such recipient is required to repay reimbursement funds under subsection (b)(1)(A).

SEC. 7. DEFINITIONS.

In this Act:

(1) ADVANCED COMMUNICATIONS SERVICE.—The term ''advanced communications service'' has the meaning given the term ''advanced telecommunications capability'' in section 706 of the Telecommunications Act of 1996 (47 U.S.C. 1302).

(2) COMMISSION.—The term ''Commission'' means the Federal Communications Commission.

(3) COVERED COMMUNICATIONS EQUIPMENT OR SERVICE.—The term ''covered communications equipment or service'' means any communications equipment or service that is on the list published by the Commission under section 2(a).

(4) CUSTOMERS.—The term ''customers'' means, with respect to a provider of advanced communications service—

(A) the customers of such provider; and

(B) the customers of any affiliate (as defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153)) of such provider.

(5) EXECUTIVE BRANCH INTERAGENCY BODY.—The term ''executive branch interagency body'' means an interagency body established in the executive branch.

(6) FEDERAL AGENCY.—The term ''Federal agency'' has the meaning given the term ''agency'' in section 551 of title 5, United States Code.

(7) FEDERAL FUNDS.—The term ''Federal funds'' means—

(A) funds from a Federal universal service support program established under section 254 of the Communications Act of 1934 (47 U.S.C. 254);

(B) any other Federal grants, subsidies, or loans to support the deployment of communications networks in the United States; and

(C) any private loans—

(i) the purpose of which is to support the deployment of communications networks in the United States; and

(ii) that are—

(I) obtained using a loan guarantee from the Federal Government; or

(II) secured in whole or in part by other funds from the Federal Government.

(8) PERSON.—The term ''person'' means an individual or entity.

(9) PROGRAM.—The term ''Program'' means the Secure and Trusted Communications Networks Reimbursement Program established under section 4(a).

(10) PROVIDER OF ADVANCED COMMUNICATIONS SERVICE.—The term ''provider of advanced communications service'' means a person who provides advanced communications service to United States customers.

(11) RECIPIENT.—The term ''recipient'' means any provider of advanced communications service the application of which for a reimbursement under the Program has been approved by the Commission, re-

gardless of whether the provider has received reimbursement funds.

(12) REIMBURSEMENT FUNDS.—The term ''reimbursement funds'' means any reimbursement received under the Program.

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. 4461

To direct the Secretary of Homeland Security to establish a program to share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. KINZINGER (for himself and Mr. MICHAEL F. DOYLE of Pennsylvania) introduced the following bill; which was referred to the Committee on

---

A BILL

To direct the Secretary of Homeland Security to establish a program to share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Network Security Information Sharing Act of 2019".

SEC. 2. INFORMATION SHARING WITH TRUSTED PROVIDERS OF ADVANCED COMMUNICATIONS SERVICE AND TRUSTED SUPPLIERS OF COMMUNICATIONS EQUIPMENT OR SERVICES.

(a) INFORMATION SHARING PROGRAM.—

(1) ESTABLISHMENT.—Not later than 120 days after the date of the enactment of this Act, including an opportunity for notice and comment, the Secretary, in cooperation with the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the Assistant Secretary, and the Commission, shall establish a program to share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services.

(2) ACTIVITIES.—In carrying out the program established under paragraph (1), the Secretary shall—

(A) conduct regular briefings and other events to share information with trusted providers of advanced communications service and trusted suppliers of communications equipment or services;

(B) engage with trusted providers of advanced communications service and trusted sup-

pliers of communications equipment or services, in particular such providers and suppliers that—

(i) are small businesses; or

(ii) primarily serve rural areas;

(C) not later than 180 days after the date of the enactment of this Act, submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a plan for—

(i) declassifying material, when feasible, to help share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services; and

(ii) expediting and expanding the provision of security clearances to facilitate information sharing regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services; and

(D) ensure that the activities carried out through the program are consistent with and, to the extent practicable, integrated with, ongoing activities of the Department of Homeland Security and the Department of Commerce.

(3) SCOPE OF PROGRAM.—The program established under paragraph (1) shall involve only the sharing of information regarding supply chain security risks by the Federal Government to trusted providers of advanced communications service and trusted suppliers of communications equipment or services, and not the sharing of such information by such providers and suppliers to the Federal Government.

(4) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this subsection $50,000,000 for fiscal year 2020. Such amounts are authorized to remain available through fiscal year 2025.

(b) REPRESENTATION ON CSRIC OF INTERESTS OF PUBLIC AND CONSUMERS.—

(1) IN GENERAL.—The Commission shall appoint to the Communications Security, Reliability, and Interoperability Council (or any successor thereof), and to each subcommittee, workgroup, or other

subdivision of the Council (or any such successor), at least one member to represent the interests of the public and consumers.

(2) INITIAL APPOINTMENTS.—The Commission shall make the initial appointments required by paragraph (1) not later than 180 days after the date of the enactment of this Act. Any member so appointed shall be in addition to the members of the Council, or the members of the subdivision of the Council to which the appointment is being made, as the case may be, as of the date of the enactment of this Act.

(c) DEFINITIONS.—In this section:

(1) ADVANCED COMMUNICATIONS SERVICE.—The term ''advanced communications service'' has the meaning given the term ''advanced telecommunications capability'' in section 706 of the Telecommunications Act of 1996 (47 U.S.C. 1302).

(2) ASSISTANT SECRETARY.—The term ''Assistant Secretary'' means the Assistant Secretary of Commerce for Communications and Information.

(3) COMMISSION.—The term ''Commission'' means the Federal Communications Commission.

(4) COMMUNICATIONS EQUIPMENT OR SERVICE.—The term ''communications equipment or serv-

ice'' means any equipment or service that is essential to the provision of advanced communications service.

(5) FOREIGN ADVERSARY.—The term ''foreign adversary'' means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

(6) PERSON.—The term ''person'' means an individual or entity.

(7) PROVIDER OF ADVANCED COMMUNICATIONS SERVICE.—The term ''provider of advanced communications service'' means a person who provides advanced communications service to United States customers.

(8) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(9) SUPPLY CHAIN SECURITY RISK.—The term ''supply chain security risk'' includes specific risk and vulnerability information related to equipment and software.

(10) TRUSTED.—The term ''trusted'' means, with respect to a provider of advanced communications service or a supplier of communications equipment or service, that the Secretary has determined

that such provider or supplier is not owned by, controlled by, or subject to the influence of a foreign adversary.

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. 4462

To amend the National Telecommunications and Information Administration Organization Act to provide for the establishment of an electromagnetic spectrum sharing research and development program and an integrated spectrum automation enterprise strategy, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. MICHAEL F. DOYLE of Pennsylvania (for himself and Mr. LATTA) introduced the following bill; which was referred to the Committee on

---

A BILL

To amend the National Telecommunications and Information Administration Organization Act to provide for the establishment of an electromagnetic spectrum sharing research and development program and an integrated spectrum automation enterprise strategy, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Studying How to Harness Airwave Resources Efficiently Act of 2019" or the "SHARE Act".

SEC. 2. NTIA ELECTROMAGNETIC SPECTRUM SHARING RESEARCH AND DEVELOPMENT PROGRAM AND STRATEGY.

Part A of the National Telecommunications and Information Administration Organization Act (47 U.S.C. 901 et seq.) is amended by adding at the end the following:

"SEC. 106. ELECTROMAGNETIC SPECTRUM SHARING RESEARCH AND DEVELOPMENT PROGRAM AND STRATEGY.

"(a) RESEARCH AND DEVELOPMENT PROGRAM.—Not later than 1 year after the date of the enactment of the Studying How to Harness Airwave Resources Efficiently Act of 2019, the Assistant Secretary, in consultation with the Commission, shall establish a program to research and develop innovative technologies and techniques that facilitate the sharing of the same covered electromagnetic spectrum by more than one Federal entity.

"(b) DEVELOPMENT OF INTEGRATED SPECTRUM AUTOMATION ENTERPRISE STRATEGY.—

"(1) IN GENERAL.—Not later than 1 year after the date of the enactment of the Studying How to

Harness Airwave Resources Efficiently Act of 2019, the Assistant Secretary, in consultation with the Commission, shall propose, after notice and opportunity for comment, an integrated spectrum automation enterprise strategy to address the management of covered electromagnetic spectrum in order to facilitate the sharing of such spectrum by more than one Federal entity.

"(2) MATTERS ENCOMPASSED.—In developing the strategy under paragraph (1), the Assistant Secretary shall consider, at a minimum, whether to propose—

"(A) changes in policy or to the law, including legislative and regulatory changes; and

"(B) using—

"(i) databases;

"(ii) artificial intelligence;

"(iii) spectrum management processes;

"(iv) public-facing application programming interfaces and online tools;

"(v) automatic frequency coordination systems;

"(vi) spectrum enforcement requirements;

"(vii) listen-before-talk;

"(viii) environmental sensing capabilities; and

"(ix) electromagnetic spectrum compatibility analyses.

"(3) ESTABLISHMENT OF SHARING TEST BED.—Not later than 15 months after the date of the enactment of the Studying How to Harness Airwave Resources Efficiently Act of 2019, the Assistant Secretary, in consultation with the Commission, shall, as part of the strategy proposed under paragraph (1), establish at least one test bed to demonstrate the potential for automated technologies to facilitate the sharing of the same covered electromagnetic spectrum by more than one Federal entity.

"(4) UPDATES TO STRATEGY.—Not later than 1 year after the strategy under paragraph (1) is proposed, and annually thereafter, the Assistant Secretary shall update such strategy.

"(c) REPORT.—Not later than 18 months after the date of the enactment of the Studying How to Harness Airwave Resources Efficiently Act of 2019, and annually thereafter, the Assistant Secretary, in consultation with the Commission, shall submit to the Committee on Energy and Commerce of the House of Representatives and the

Committee on Commerce, Science, and Transportation of the Senate a report containing—

"(1) the results of the program established under subsection (a); and

"(2) the strategy proposed under subsection (b)(1) with respect to the first report submitted under this subsection and updates to the strategy proposed under such subsection with respect to reports submitted thereafter.

"(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Assistant Secretary to carry out this section $50,000,000 for fiscal year 2020. Such amounts are authorized to remain available until expended.

"(e) DEFINITIONS.—In this section:

"(1) COVERED ELECTROMAGNETIC SPECTRUM.—The term 'covered electromagnetic spectrum' means electromagnetic spectrum allocated for exclusive or primary use by Federal entities.

"(2) FEDERAL ENTITY.—The term 'Federal entity' has the meaning given such term in section 113(l).".

SEC. 3. FEDERAL COMMUNICATIONS COMMISSION REPORT ON EXPANDING SPECTRUM SHARING TECHNIQUES.

(a) REPORT.—Not later than 12 months after the first assignment of Priority Access Licenses through the system of competitive bidding, after an opportunity for notice and comment, the Federal Communications Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that assesses and provides recommendations for expanding upon and improving spectrum sharing techniques developed for use in the 3.5 gigahertz band and that includes the following considerations:

(1) How to promote an ecosystem of devices employing such sharing techniques.

(2) How to ensure that any Federal protection zones and corresponding technical rules and power levels are no more protective than necessary.

(3) The applicability of such sharing techniques to frequencies between 3100 megahertz and 3550 megahertz, inclusive, and frequencies between 7125 megahertz and 8400 megahertz, inclusive, to the extent any portion of such frequencies cannot be cleared in a reasonable amount of time.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a)(3) may be construed to require that every spectrum sharing technique developed for use in the 3.5 gigahertz band be recommended for use in other bands.

.....

(Original Signature of Member)

116TH CONGRESS
1ST SESSION

H. R. 4500

To direct the Assistant Secretary for Communications and Information to take certain actions to enhance the representation of the United States and promote United States leadership in communications standards-setting bodies, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. WALBERG introduced the following bill; which was referred to the Committee on _____

A BILL

To direct the Assistant Secretary for Communications and Information to take certain actions to enhance the representation of the United States and promote United States leadership in communications standards-setting bodies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Promoting United States Wireless Leadership Act of 2019".

SEC. 2. REPRESENTATION AND LEADERSHIP OF UNITED STATES IN COMMUNICATIONS STANDARDS-SETTING BODIES.

(a) IN GENERAL.—In order to enhance the representation of the United States and promote United States leadership in standards-setting bodies that set standards for 5G networks and for future generations of wireless communications networks, the Assistant Secretary shall, in consultation with the National Institute for Standards and Technology, coordinate executive branch efforts to—

(1) encourage participation by trusted companies and a wide variety of relevant stakeholders (to the extent such standards-setting bodies allow such stakeholders to participate) in such standards-setting bodies; and

(2) offer technical expertise to trusted companies and a wide variety of relevant stakeholders (to the extent such standards-setting bodies allow such stakeholders to participate) to facilitate such participation.

(b) STANDARDS-SETTING BODIES.—The standards-setting bodies referred to in subsection (a) include, but is not limited to—

(1) the International Organization for Standardization;

(2) the voluntary standards-setting bodies that develop protocols for wireless devices and other equipment, such as the 3GPP and the Institute of Electrical and Electronics Engineers; and

(3) any standards-setting body accredited by the American National Standards Institute or Alliance for Telecommunications Industry Solutions.

(c) BRIEFING.—Not later than 60 days after the date of the enactment of this Act, the Assistant Secretary shall brief the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate on a strategy to carry out subsection (a).

(d) DEFINITIONS.—In this section:

(1) 3GPP.—The term "3GPP" means the 3rd Generation Partnership Project.

(2) 5G NETWORK.—The term "5G network" means a fifth-generation mobile network as described by 3GPP Release 15 or higher.

(3) ASSISTANT SECRETARY.—The term "Assistant Secretary" means the Assistant Secretary for Communications and Information.

(4) CLOUD COMPUTING.—The term "cloud computing" has the meaning given the term in Special Publication 800–145 of the National Institute of

Standards and Technology, entitled "The NIST Definition of Cloud Computing", published in September 2011, or any successor publication.

(5) COMMUNICATIONS NETWORK.—The term "communications network" means any of the following:

(A) A system enabling the transmission, between or among points specified by the user, of information of the user's choosing.

(B) Cloud computing resources.

(C) A network or system used to access cloud computing resources.

(6) TRUSTED COMPANY.—The term "trusted company" means a company that is determined by the Assistant Secretary not to pose a threat to the national security of the United States. In making such a determination, the Assistant Secretary shall consult the heads of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) and consider whether such company is listed on the entity list maintained by the Bureau of Industry and Security of the Department of Commerce and set forth in Supplement No. 4 to part 744 of the Export Administration Regula-

tions (subchapter C of chapter VII of title 15, Code of Federal Regulations).

TPG says community health fears stopped its 5G rollout in Australia – as experts blame disinformation campaigns on social media

September 19, 2019

17 September 2019 | by Jack Derwin | Business Insider |


TPG says community health fears stopped its 5G rollout in Australia – as experts blame disinformation campaigns on social media

BI Jack Derwin
Business Insider 17 September 2019

- **TPG chief operating executive Craig Levy has told the Federal Court that the telco pulled its plans to roll out a 5G network in Australia due to community fears regarding the health impact of the technology.**
- **Those fears have spiked despite bodies such as the World Health Organisation (WHO) stating there should be no risks to public health. In fact, 5G radiation should actually be safer than previous networks, according to research by Cornell University.**
- **Despite the science however, a small segment of the community appears concerned over the technology, as the number of social media groups spreading disinformation grow, galvanising opposition to the network.**

Australia has an unfortunate and chequered history of politics scuppering its national technology infrastructure.

The National Broadband Network (NBN) was kneecapped by a change of federal government and policy and has been a veritable trainwreck ever since.

In 2018, fears of Chinese espionage dashed Huawei's bid to help roll out the 5G network here. Now TPG is having to explain why it scrapped its own 5G aspirations and it appears its hand was forced – at least in part – by fears from the community about health impacts of the technology.

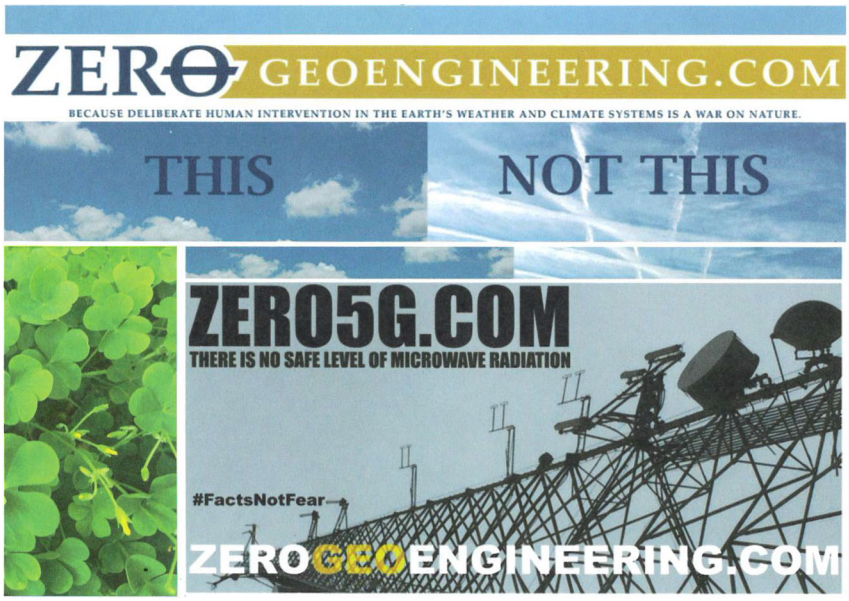
"If people have concerns about the impact on their health... they are not just looking at our model in a positive manner," chief operating executive Craig Levy told the Federal Court on Tuesday, as reported by the Sydney Morning Herald.

TPG is in court fighting its blocked attempt by the ACCC to merge with Vodafone, and inadvertently, the case rests on whether or not TPG would build the important infrastructure without a merger going forward. The telco has flatly claimed it wouldn't, so far citing a lack of commercial viability, and now community opposition.

- **TPG chief operating executive Craig Levy has told the Federal Court that the telco pulled its plans to roll out a 5G network in Australia due to community fears regarding the health impact of the technology.**

Link To Full Article

Articles


ZERO GEOENGINEERING.COM
BECAUSE DELIBERATE HUMAN INTERVENTION IN THE EARTH'S WEATHER AND CLIMATE SYSTEMS IS A WAR ON NATURE.
THIS
NOT THIS
ZERO5G.COM
THERE IS NO SAFE LEVEL OF MICROWAVE RADIATION
#FactsNotFear
ZEROGEOENGINEERING.COM

Have you looked at the sky lately? The lingering emissions pollution spewed by jets isn't just water vapor. Recent rain and snow sample lab reports indicate the Geoengineering "footprint" is visible around the world, present due to the ongoing development and use of Geoengineering and Weather Modification, deliberate large-scale human interventions to change Earth's weather and climate systems.

ZERO GEOENGINEERING.COM

BECAUSE DELIBERATE HUMAN INTERVENTION IN THE EARTH'S WEATHER AND CLIMATE SYSTEMS IS A WAR ON NATURE

Deliberate human manipulation of the Earth's weather and climate systems is a war on Nature and All Life on Earth.

WE DO NOT CONSENT!

GEOENGINEERING + WEATHER MODIFICATION
= MAN-MADE CLIMATE CHANGE

ZEROGEOENGINEERING.COM

International Association of Fire Chiefs
4795 Meadow Wood Lane, Suite 100 • Chantilly, VA 20151
Tel: 703.273.0911 • Fax: 703.273.9363 • IAFC.org

September 27, 2019

The Honorable Mike Doyle.
Chairman.
Committee on Energy and Commerce.
Subcommittee on Communications.
and Technology.
306 Cannon House Office Building
Washington, D.C. 20151

The Honorable Bob Latta
Ranking Member
Committee on Energy and Commerce
Subcommittee on Communications
and Technology
2467 Rayburn House Office Building
Washington, D.C. 20151

Dear Chairman Doyle and Ranking Member Latta:

Thank you for the opportunity to submit a statement for the record for today's hearing on legislating to secure America's wireless future on behalf of the International Association of Fire Chiefs.

Communications are an integral part of emergency response. For decades, land-mobile radio communications have enabled responders to speak to one another in extreme conditions like fires, hurricanes, and other natural disasters. Radio remains a central part of the public safety communications ecosystem, which has recently grown to include broadband, data, 5G and the Internet of Things (IoT).

New communications technologies hold tremendous potential for public safety. Data from IoT devices, whether coming from a smartwatch, drone, or device on a firefighter's gear, will enable us to respond smarter, faster, and more safely. We have experienced instances of smart watches detecting falls and contacting 911. Sensors on drones help us detect hot spots, enabling us to predict the path of a wildland fire. According to the National Public Safety Telecommunications Council, "with analytics, IoT data and capabilities can be combined, filtered, and analyzed to provide 'actionable intelligence' for the first responder."[1]

The First Responder Network Authority (FirstNet) is conducting important work to enable true priority and preemption for public safety wireless communications through the buildout of a national broadband network. This buildout is anticipated to be completed between 2022 and 2023 and will ensure secure and reliable network access on scene. Greater network reliability and the arrival of 5G will support telehealth initiatives, connecting EMS patients and rural communities to doctors faster. In almost every arena

[1] National Public Safety Telecommunications Council, "Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes," June 2019, Page 1.

of emergency response, connectivity and data offer exciting opportunities to improve the safety of citizens and first responders.

With the emergence of new communications capabilities come new challenges in spectrum management. The fire and emergency service uses spectrum for mission-critical communications. As Congress and the FCC push for more efficient spectrum usage, we believe it is important that mission-critical communications are protected. For example, public safety uses point-to-point microwave links in the 6 GHz band that are highly sensitive to interference and require 99.999% or 99.9999% reliability. As the FCC considers allowing unlicensed devices in the 6 GHz band in its proposed rulemaking, we strongly advocate for rigorous, government-run testing of sharing technologies so that incumbent users are protected.

Another critical issue facing public safety is the pending auction of the T-Band spectrum. The T-Band, which sits between 470-512 MHz on the electromagnetic spectrum, supports radio communications in our nation's most populated metropolitan areas. Section 6103 of Public Law 112-96 directs the FCC to auction off the public safety spectrum by February 2021.

In June, the U.S. Government Accountability Office (GAO) released a report evaluating the challenges public safety would face if forced to move off the spectrum. The report concluded that it would cost close to $6 billion to move public safety users – a figure which did not account for infrastructure investments and the testing of new equipment. As a result of its findings, the GAO concluded, "Congress should consider legislation allowing public safety users continued use of the T-Band spectrum."[2]

Congressional action on the T-Band is imperative to protecting America's emergency preparedness. Of the eleven cities using the spectrum, New York City and Boston areas rely on the band for public safety communications interoperability and resilience. In the Houston area, industrial responders and refineries use the band to keep U.S. energy assets and neighboring communities safe. In Philadelphia, the spectrum helps keep local public safety agencies and the port connected. These are merely some of the major areas that face the threat of moving their public safety communications to alternate spectrum, which, depending on the region, is likely not available. We urge the Committee to act by marking up H.R. 451 Don't Break Up the T-Band Act, co-sponsored by Representatives Eliot Engel (D, NY-16) and Lee Zeldin (R, NY-1).

Public safety relies upon dependable spectrum resources to serve America's communities. As the Committee considers spectrum legislation, I urge you to consider ways to support the public safety communications ecosystem. This involves exploring rigorous testing of spectrum sharing solutions; encouraging communications interoperability and security; supporting investment in 911 infrastructure; and providing research funds to explore the uses of communications technology in the fire and emergency services. Thank you for the opportunity to comment in this matter.

[2] U.S. Government Accountability Office, "Emergency Communications: Required Auction of Public Safety Spectrum Could Harm First Responder Capabilities," June 2019.

Sincerely,

Fire Chief Gary Ludwig, EMT-P
President and Chairman of the Board

:ba

Ms. Bobbie Stempfley

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Secure America's Wireless Future"
September 27, 2019

Ms. Bobbie Stempfley, Managing Director, CERT Division
Software Engineering Institute, Carnegie Mellon University

The Honorable Anna G. Eshoo (D-CA)

1. **Please explain the role encryption plays in protecting the American people from potential vulnerabilities in telecommunications equipment. To what degree does the encrypting of calls and internet traffic mitigate risks related to potential vulnerabilities in telecommunications equipment?**

Response: Encryption technologies are an important part of protecting the content of the communications passing across telecommunications equipment, enabling confidentiality of the message in transit. While encryption solutions can be employed to reduce the risk of eavesdropping, they are limited in their ability to reduce the risks of other vulnerabilities in the supply chain. Vulnerabilities within the supply chain could allow for attacks that alter the way the telecommunication equipment accepts, routes, and processes communications (calls, messages, video, and data). This would enable an adversary to interject content into the message stream, disrupt the transmission of content, and/or affect the timing of the distribution of content. Further, impacting the routing would also facilitate the collection of routing information, as meta-data this provides rich insight into the relationships between individuals in the communication stream and can provide insights into the nature of the communications and possible transactions.

Attachment—Additional Questions for the Record

Ms. Bobbie Stempfley, Managing Director, CERT Division
Software Engineering Institute, Carnegie Mellon University

The Honorable Tim Walberg (R-MI)

1. **We recognize the concerns that rural carriers like Pine Belt, with their limited budgets, have when it comes to complying with the reimbursement program while also trying to deploy new, or upgrade existing, networks.**

    a. **Are there certain types of network equipment or services that are particularly vulnerable that should be prioritized for removal?**

Response: If the focus is to provide risk reduction, prioritization should not be on type of equipment, i.e. replace all routers before the switches, etc., rather it should be on the key places and roles of the equipment in the infrastructure. In any telecommunications architecture the equipment that provides the core management and infrastructure sits in a privileged place in the architecture. In this instance the elements of the transport that support the radio access network and the services that are required to provide the routing and peering point services should be prioritized.

Mr. John Nettles

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Secure America's Wireless Future"
September 27, 2019

Mr. John Nettles, President, Pine Belt Wireless

The Honorable Robert E. Latta (R-OH)

1. **Mr. Nettles: We've heard from several smaller, rural providers who won Universal Service Funding who are concerned about accepting their award. In some cases, they won competitive bids using underpriced, potentially vulnerable equipment. H.R. 4459 attempts to allow an "out" for those who know they won't be able to comply with the law and still meet buildout obligations with secure, but potentially more expensive equipment. How critical is this "hold harmless" provision, and how important is clarity from the FCC on what vendors are acceptable to use in the future without risk of unintended consequences?**

Response: Clarity with respect to the question of a vendor's acceptability is absolutely critical. Carriers need certainty when making purchasing decisions for network deployments, maintenance and upgrades, and services and support. Equipment and software purchases are investments in our networks that have long term implications. To say only who we are not allowed to purchase from could be likened to sending someone to navigate a maze with the lights out and eyes blindfolded. To the extent there is a "black list' of equipment providers, it is essential for all carriers to have necessary information regarding what providers are deemed secure.

Regarding the "hold harmless" provision, for the build-out requirements, Pine Belt's wireline operation is already built-out with vendor equipment that is not a subject of the supply chain security debates. As such, I can only speculate as to its importance but I believe that too is very high. It is almost a certainty that those who bid on the funds for broadband buildout did so using known costs from their current infrastructure base. If their current vendor is deemed a security risk and prohibited, bid winners would need to replace their base equipment first before moving into the service buildout stage. This would most assuredly have an impact on both the operators financial and time estimates. Carriers should not be held in default and penalized for no longer being able to meet the terms of a bid because of changed circumstances regarding allowed equipment providers.

Attachment—Additional Questions for the Record

Mr. John Nettles, President, Pine Belt Wireless

The Honorable Susan W. Brooks (R-IN)

1. **How long do you believe it would take you to replace the Huawei equipment in your network, provided you had all the replacement equipment you needed on hand?**

Response: To clarify, we have ZTE equipment in our wireless network. Notwithstanding that detail, reflecting on our Mobility Phase I buildout requirements and experience, it took us approximately 28 months to move through a very deliberate vendor selection process, install a new core, construct 13 new tower sites and retrofit another 40 plus sites. Given that our site count has grown since then and assuming the replacement would involve both the core and the radio access network, I would estimate that the replacement work could be completed in a 36 to 42 month timeframe. This estimate is subject to change based on what network components must be replaced; if only core equipment or equipment capable of switching packets must be replaced, the timeframe could be shorter.

2. **How long does it typically take to fulfill an order when you purchase network equipment from a supplier?**

Response: Depending on the type and quantities, it can be anywhere from a few weeks to several months. For small quantities of items that had been previously deployed and for which a configuration template or example exists for the specifics of our network requirements, ZTE always quoted us no less than a twelve-week delivery window. For something like a core replacement, the delivery window will often be 90 to 120 days. However, the "long pole in the tent" is a sequence of events that starts with what is generally called "rack, stack and powering," something that can take two to four weeks, followed by initial commissioning, configuration and translations, integration with connecting network segments and culminating with data migration and service conversion. These steps can take anywhere from three to nine months or longer. The point being that the physical order fulfilment is only one element of the time requirement. Likewise, for a core replacement, the work is generally done at a single physical location with the majority of the time being spent on software tasks. When one moves to the radio access network, given that each site is a unique physical location, staging and transport of items from site to site becomes a time impacting factor as well.

Further, smaller carriers serving rural areas lack the economies of scale of the largest wireless providers, and could be subject to delays based on availability constraints flowing from equipment purchasing decisions of the nationwide carriers. In other words, if I order 40 units of a component from Preferred Vendor A and one of the nationwide carriers orders 400 at or about the same time with 400 more expected in the near term, my order will likely suffer in terms of delivery time.

Attachment—Additional Questions for the Record

Mr. John Nettles, President, Pine Belt Wireless

The Honorable Tim Walberg (R-MI)

1. **We recognize the concerns that rural carriers like Pine Belt, with their limited budgets, have when it comes to complying with the reimbursement program while also trying to deploy new, or upgrade existing, networks.**

    a. **If this program is enacted into law, how would Pine Belt manage the need to remove suspect equipment while also trying to maintain network buildout and upgrades?**

Response: With only a few exceptions, our network expansion and upgrades have been on hold for the past 12 months pending resolution of this issue. So, it will be essential for us to select our replacement vendor first and then order, receive, install, commission, integrate and convert to the replacement equipment. Once these steps are complete, we would then resume network expansion and upgrade efforts. Decommissioning and removal of the suspect equipment could and most likely would be done in parallel with resumption of our expansion and upgrade activities. Overall, to prevent cutting off service to customers in rural America, we must focus on "replace then rip" instead of "rip and replace."

    b. **Are there certain types of network equipment or services that are particularly vulnerable that should be prioritized for removal?**

Response: If you segment the network into the four linear elements of user equipment, radio access, backhaul and core, it seems to me that the two outer segments, user equipment and the core, would be those most susceptible to security vulnerabilities.

2. **You mentioned that small carriers lack economies of scale, making it difficult for trustworthy network suppliers to be competitive in price. What are your thoughts on allowing several small carriers to join together in placing orders to help achieve scale replacement?**

Response: This is something that sounds like a good idea. As with nearly anything, however, the devil will be within the details and I am struggling to see how, when it comes to network gear, something of this sort would be managed from a practical matter. A system could be developed that provided for sanctioned pricing from preferred vendors with the carriers having the option of purchasing from "the list" or trying to negotiate outside the system. One of the challenges I see in something like this would be that of confidentiality between vendors.

    a. **Is this something Pine Belt would consider participating in?**

Response: If it created a real equipment cost advantage with minimal administrative cost and limited contingent liabilities and other risks, absolutely.

Mr. Harold Feld

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Secure America's Wireless Future"
September 27, 2019

Mr. Harold Feld, Senior Vice President, Public Knowledge

The Honorable Anna G. Eshoo (D-CA)

1. **The Prague Proposals appear to be a good first step in outlining a framework for how countries should think about network security as we transition to 5G. Please explain why this agreement is important, what it accomplishes, and where it falls short.**

Response: The Prague Proposals are important because they provide a sensible framework for international norms on cybersecurity, balanced with respect for principles of free trade. Numerous trade agreements contain telecommunications chapters that prohibit discrimination against telecommunications equipment providers or service providers. The Prague Proposals recognize that the potential influence of third-party countries on providers should be considered when weighing cybersecurity concerns.

The provision of the Prague Proposals on "the economy" may have impact on programs to fund deployment of broadband networks, or require changes in the financial oversight of 5G network providers. Existing SEC filings which do not require financial management of 5G networks to be broken out separately, or 5G network deployments by non-publicly traded companies, may not comply with the Prague Proposal requirement for "transparent" financial records. As with all broad statement of principles, much will depend on implementation.

Attachment—Additional Questions for the Record

Mr. Harold Feld, Senior Vice President, Public Knowledge

The Honorable Yvette D. Clarke (D-NY)

1. **As we think about encouraging the development of new technology, services, and millions of IoT devices that will transform our communities into 21st Century 'Smart Cities':**

    a. **Mr. Feld, how critical will it be for policymakers to identify new spectrum that can support unlicensed operations?**

Response: Identifying new spectrum for unlicensed use, particularly spectrum capable of supporting large, contiguous channels, is critical both to achieving future economic growth and innovation in wireless connectivity and even to simply maintaining the high level of connectivity available today. As an initial matter, the exponential increase in the number of devices connecting through unlicensed protocols such as Wi-Fi and Bluetooth, and the demand for low-cost access and flexibility to create custom-designed networks, increasingly strain the capacity of existing unlicensed bands. In crowded urban environments in particular, the rise of home networks and proliferation of "smart" devices requires greater unlicensed access in the same way that the rise in mobile broadband through cellular services requires greater access to licensed spectrum. Indeed, it is a tribute to the innovative strength of the unlicensed equipment industry that the existing allocations of unlicensed spectrum support the enormous amount of activity we rely on daily for everything from the trivial to life saving technologies.

Looking to the future, unlocking the true value of the 5G revolution requires significant expansion of unlicensed spectrum. It is well documented that the rise of 4G networks was made possible through the synergistic combination of licensed spectrum and unlicensed spectrum.[1] Specifically, licensed networks are dependent on "Wi-Fi hand off" to balance load and capacity, and without the availability of Wi-Fi licensed 4G would have collapsed under the weight of its own demand.[2] Unlicensed spectrum has also proven to be an indispensable tool for bringing affordable broadband to rural areas and poorer urban communities, where carriers using licensed spectrum do not find the rate of return sufficient to deploy.[3] We can expect a similar synergy for

---

[1] *See, e.g.,* Mark Cooper, "Efficiency Gains and Consumer Benefits of Unlicensed Access to the Public Airwaves," (2012) available at: https://ecfsapi.fcc.gov/file/7521479487.pdf

[2] Mark Cooper, "The Consumer Benefits of Expanding Shared use of Unlicensed Radio Spectrum: Liberating Long-Term Spectrum Policy From Short Term Thinking," (2011) Available at: https://consumerfed.org/pdfs/Consumer-Benefits-of-Shared-Use-Spectrum.pdf

[3] *See* Carl Weinschenk, "Latest Airband Project: Microsoft, ARK Multicasting Seek To Ease Rural Congestion," Telecompetitor (October 15, 2015). Availabe at:

unlicensed spectrum and licensed spectrum in 5G, amplified by the greater capacities of new technology developed over the last decade.

In particular, the allocation of wide swaths of new spectrum for unlicensed use, such as the proposed used of the 6 GHz band, is critical to the success of Wi-Fi 6. Like the licensed 5G protocol (3GPP Release 15), Wi-Fi 6 is about much more than simply boosting speed (although it does that as well). Wi-Fi 6 has been optimized to support a vastly larger number of connected devices, providing necessary support for the rise of IoT.[4] To function effectively, however, Wi-Fi 6 requires greenfield spectrum for deployment – and specifically greenfield spectrum capable of supporting large, contiguous channel blocks for maximum efficiency.

In short, opening new spectrum for unlicensed use will supercharge our 5G deployment and may provide a key advantage in our "race to 5G" against countries such as China that have no unlicensed strategy. By contrast, failure to make new spectrum available for unlicensed access will deprive us of a crucial component for 5G success.

b. How do you see unlicensed technologies supporting the development of Smart Cities?

Response: Unlicensed access supports the development of smart cities in several ways. First, enhanced unlicensed access provides flexibility for cities to customize their IoT and other networks to their specific needs, without the need to find a licensee willing to contract with them for each project and purpose. Second, unlicensed spectrum reduces the price of developing smart technology dramatically by reducing the transaction cost of contracting with a licensee, and by generating economies of scale in the equipment market.

Additionally, the availability of unlicensed spectrum access allows cities to migrate traffic that does not require the interference protection of licensed spectrum to unlicensed spectrum. This frees licensed spectrum for more sensitive traffic, enhancing overall spectrum efficiency. By matching the nature of the traffic with the appropriate level of interference protection, cities can ensure sufficient spectrum access for a wide range of projects that would simply not be achievable through reliance on licensed spectrum alone.

Smart cities, or smart roads or smart homes or smart anything for that matter, rely on unlicensed access. Already our would of connected devices assumes access through an unlicensed connection, creating a demand that has brought the price for Wi-Fi chips down to almost

---

https://www.telecompetitor.com/latest-airband-project-microsoft-ark-multicasting-seek-to-ease-rural-isp-network-congestion/?utm_source=sendgrid&utm_medium=email&utm_campaign=Newsletters&mc_cid=fb6e9480db&mc_eid=bf11efc24c

[4] *See* Jacob Kasternakes, "Wi-Fi 6: Is It Really That Much Faster?" The Verge (February 21, 2019). Available at: https://www.theverge.com/2019/2/21/18232026/wi-fi-6-speed-explained-router-wifi-how-does-work

nothing. To continue this connected revolution, Congress and the FCC must ensure an adequate supply of quality unlicensed spectrum – both in the short term and in the "pipeline" for the long term.

Mr. Dean R. Brenner

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"Legislating to Secure America's Wireless Future"
September 27, 2019

Mr. Dean R. Brenner, Senior Vice President
Spectrum Strategy & Tech Policy, Qualcomm Incorporated

The Honorable Anna G. Eshoo (D-CA)

1. **Please explain the role encryption plays in protecting the American people from potential vulnerabilities in telecommunications equipment. To what degree does the encrypting of calls and internet traffic mitigate risks related to potential vulnerabilities in telecommunications equipment?**

Response: As I discussed in my testimony, security of the entire cellular communications system is a top priority for Qualcomm. To that end, Qualcomm is working, and often leading, several activities in this area. From the perspective of ensuring security of the underlying cellular technology, Qualcomm is actively involved in 3GPP, the leading organization responsible for the 4G and 5G global standards. Also, as stated in my testimony, one of our engineers, Dr. Farrokh Khatibi, was appointed to lead the FCC CSRIC VII Working Group on Managing Security Risk in Emerging 5G Implementations.

In addition, Qualcomm is engaged in activities to ensure supply chain risk management. An example of this effort is the work taking place in the ATIS (Alliance for Telecommunications Industry Solutions) 5G Supply Chain Working Group in collaboration with the Department of Defense. The aforementioned FCC CSRIC VII is also working on supply chain security. These efforts include the development and standardization of several important techniques to ensure the security of communications systems, including mutual authentication, encryption, and integrity protection.

All of these activities are aimed at protecting the American people from any potential vulnerabilities in the cellular communications system.

Attachment—Additional Questions for the Record

Mr. Dean R. Brenner, Senior Vice President
Spectrum Strategy & Tech Policy, Qualcomm Incorporated

The Honorable Yvette D. Clarke (D-NY)

1. **As you know, we are in the midst of a race to 5G.**

    a. **Mr. Brenner, given your work in this area, what are your strategy recommendations to Congress that will help us win the race?**

Response: As I stated in my testimony, ensuring a steady stream of new spectrum – low, mid, and high band; and licensed, unlicensed, and shared – is essential for the rapid, broad 5G roll-out in the U.S. Congress is to be commended for enacting legislation, such as the Mobile NOW Act, which has contributed to new spectrum availability. Going forward, it's essential that Congress continue to exercise its oversight authority to ensure the goals of the Mobile NOW Act are achieved, and to continue to pursue new legislation, such as the SHARE Act (H.R. 4462), which would encourage the development and use of advanced sharing techniques so that spectrum can be used more efficiently by the Government.

As I explained in my oral testimony, I believe that Section 2 of the SHARE Act should be amended to include two additional tools: "Look Before Talk" and "Synchronization." Use of these additional tools, which take advantage of the speed of the new 5G radios and the improved directionality of 5G transmissions using narrow beams, can produce better, faster mobile broadband, as well as power savings for mobile devices.

    b. **What are your recommendations to the FCC? NTIA?**

Response: My recommendation to the FCC is to continue to press forward in making new spectrum available for 5G. This effort should include, in addition to the upcoming millimeter wave auctions, making the entire 6 GHz band available for unlicensed use, and allowing C-V2X to have access to a portion of the 5.9 GHz spectrum. Qualcomm's specific recommendations to the FCC on these topics are available here and here.

My recommendation to the NTIA, as described in my testimony, is to continue to serve as the lead coordinator between federal agencies and the private sector on spectrum sharing. It's critical that NTIA continue to play a coordinating role amongst these entities and to speak with a unified voice for the Executive Branch to make progress toward greater sharing. No other federal agency is capable of serving in this role, so it's paramount that NTIA continue to serve in this capacity.

2. **I personally struggle with the traffic in New York City. It has become a great challenge to solve. 5G technology is one of the solutions that is in the current conversation to make traffic flow more efficiently.**

    a. **Mr. Brenner, could you explain C2VX and the impact it would have on dense traffic areas like New York City?**

Response: C-V2X is a ground-breaking technology that has great potential to save lives, improve traffic flow in congested areas, such as New York City, and conserve energy. C-V2X enables direct, peer-to-peer communications between vehicles ("V2V"), vehicles and vulnerable persons such as pedestrians and cyclists ("V2P"), and vehicles and transportation infrastructure ("V2I"), as well as communications between vehicles and mobile networks ("V2N"). Importantly, recent testing completed by the 5G Automotive Association ("5GAA"), which is a rapidly growing global association comprising many of the world's major automotive, technology and telecommunications companies, demonstrates that the C-V2X V2V mode consistently outperforms an older technology known as DSRC in key areas such as non-line-of-sight operations, resiliency and range. Qualcomm's primary objective in designing C-V2X has been to improve road safety. However, C-V2X will also allow cities to take advantage of V2V, V2I and V2P communications to provide a variety of traffic mitigating solutions, such as traffic flow optimization, hazard protection and potential reduction in traffic rule violations. In addition, C-V2X, which will begin using 4G technology, has an evolutionary path to 5G, which will provide even greater safety and traffic efficiency benefits, including enabling robust communications for fully autonomous cars.

As mentioned in my testimony, unfortunately, current FCC rules allow only for DSRC to have access to the 5.9 GHz spectrum, the same spectrum for which C-V2X is designed. DSRC was developed over twenty years ago and does not have the performance advantages of C-V2X. Currently, no automaker has plans to deploy DSRC in the United States. Meanwhile, Ford has announced plans to deploy C-V2X in all new cars in the U.S. beginning in 2022. The 5GAA has submitted a waiver request to the FCC that, if granted, would allow C-V2X to have access to a portion of the 5.9 GHz band, while allowing DSRC to continue to have access to a separate portion of the band. In addition, 5GAA has proposed a fuller band plan for the 5.9 GHz spectrum that would accommodate 5G-based C-V2X, while also retaining the ability for DSRC to have access to the band. It is imperative that the FCC grant the 5GAA waiver request soon and consider the fuller proposal for the 5.9 GHz spectrum, which currently is under-utilized, resulting in the public being denied the safety and traffic efficiency benefits that C-V2X can provide. Absent prompt FCC action, this new technology, which could improve safety and traffic in New York City and other areas around the country, cannot be launched.

Attachment—Additional Questions for the Record

Mr. Dean R. Brenner, Senior Vice President
Spectrum Strategy & Tech Policy, Qualcomm Incorporated

The Honorable Robert E. Latta (R-OH)

1. **Mr. Brenner: The SHARE Act contemplates developing new spectrum sharing tools in the 3100-3450-megahertz band, as well as in 7 gigahertz. Would you offer your thoughts as to where NTIA should train their focus with these new tools, if enacted?**

Response: As stated in my oral testimony, the SHARE Act should be amended to include two new tools, in addition to the nine already contained in Section 2 of the bill. These two additional tools are "Look Before Talk," and "Synchronization." The technical name for look before talk is "coordinated multipoint transmission" (CoMP). Synchronization enables a technique called "spatial division multiplexing" (SDM). Use of these advanced sharing techniques, which Qualcomm has demonstrated, will increase spectrum efficiency and assist the Government in uncovering the best ways to achieve the highest utilization of scarce spectrum resources, including in the 3100-3450-megahertz band and in the 7 GHz band.

Attachment—Additional Questions for the Record

Mr. Dean R. Brenner, Senior Vice President
Spectrum Strategy & Tech Policy, Qualcomm Incorporated

The Honorable Susan W. Brooks (R-IN)

1. **Can you explain the process Qualcomm uses to ensure your products are secure from outside intrusion?**

Response: Qualcomm has recognized security as one of the key attributes of our products (chipsets and related software) since the early days of the company. Over the years, we have made significant investments to continuously improve the security of our products to counter ever-increasing cyber security threats. We believe the most effective way to approach the security of our products is to build security measures into all phases of the product development lifecycle and provide specific security trainings to our workforce. In the early product concept and design phase, we apply threat modeling to identify potential attacks and follow security design principles to build a strong security foundation. In the implementation and validation phases, we use a variety of tools and methods to prevent and detect security vulnerabilities that may appear in our products. Post product launch, our effective incident response process addresses issues reported by security researchers and attacks in the public domain, and releases security patches to our customers in a timely manner. We established our vulnerability rewards program in 2016 to work with the security research community to further improve the security of our products. We continue to be vigilant against new types of attacks on our products and continually seek ways to further improve our comprehensive and effective approach to security.

2. **How do you protect your equipment from being compromised when it is used in conjunction with ZTE or Huawei products in specific devices?**

Response: We use the same process described above with all the manufacturers (so-called OEMs) to whom we supply our products, and we have found our process to be very effective in ensuring the security of our products.

Attachment—Additional Questions for the Record

Mr. Dean R. Brenner, Senior Vice President
Spectrum Strategy & Tech Policy, Qualcomm Incorporated

The Honorable Tim Walberg (R-MI)

1. **I'm pleased to see H.R. 4500 on today's hearing, a bipartisan bill I've introduced with my fellow 5G Caucus Co-Chairs, Ms. Dingell and Ms. Brooks. In Ms. Stempfley's testimony she talked about the need to understand changes in supply chain components and systems as we move ahead in time, which inherently leads to a software or component bill of materials. NTIA currently plays a critical role coordinating how to share software bills of materials across the Federal government, promote transparency, and how to communicate vulnerabilities of components downstream in the supply chain.**

    a. **As companies like yours participate in global standards setting bodies that shape future technologies like 5G, how important is it for Qualcomm and others to have a strong partnership with the technical experts in the Federal government supporting their work in the communications standards body arena?**

Response: Qualcomm plays a lead role in standards bodies, including in 3GPP, which has developed, and continues to develop, the global 4G and 5G standards. NTIA is a regular participant in 3GPP, which unites seven telecommunications standard development organizations from around the globe and has provided a constructive environment for standards development. Other organizations from the US government that participate in 3GPP include the Federal Communications Commission, Department of Defense, the Department of Transportation, and several US government research laboratories. Within 3GPP activities, Qualcomm interacts on a regular basis with US government technical experts, and these interactions are valuable for the US government, Qualcomm, and the wireless industry writ large.

2. **You mentioned that small carriers lack economies of scale, making it difficult for trustworthy network suppliers to be competitive in price. What are your thoughts on allowing several small carriers to join together in placing orders to help achieve scale replacement?**

    a. **Do you have any thoughts on this idea?**

Response: Qualcomm does not sell core network equipment to U.S. carriers. As such, we are not the experts in this area.

○