A SAFE WIRELESS FUTURE: SECURING OUR NETWORKS AND SUPPLY CHAINS

HYBRID HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JUNE 30, 2021

Serial No. 117–41

Published for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PUBLISHING OFFICE

51–410 PDF WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

FRANK PALLONE, JR., New Jersey
Chairman

BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
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
PAUL TONKO, New York
YVETTE D. CLARKE, New York
KURT SCHRADER, Oregon
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, *Vice Chair*
NANETTE DIAZ BARRAGÁN, California
A. DONALD MCEACHIN, Virginia
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
KATHLEEN M. RICE, New York
ANGIE CRAIG, Minnesota
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas

CATHY MCMORRIS RODGERS, Washington
Ranking Member
FRED UPTON, Michigan
MICHAEL C. BURGESS, Texas
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
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
MARKWAYNE MULLIN, Oklahoma
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
JOHN R. CURTIS, Utah
DEBBBIE LESKO, Arizona
GREG PENCE, Indiana
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
KELLY ARMSTRONG, North Dakota

PROFESSIONAL STAFF

JEFFREY C. CARROLL, *Staff Director*
TIFFANY GUARASCIO, *Deputy Staff Director*
NATE HODSON, *Minority Staff Director*

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

MIKE DOYLE, Pennsylvania
Chairman

JERRY MCNERNEY, California
YVETTE D. CLARKE, New York
MARC A. VEASEY, Texas
A. DONALD MCEACHIN, Virginia
DARREN SOTO, Florida
TOM O'HALLERAN, Arizona
KATHLEEN M. RICE, New York
ANNA G. ESHOO, California
G. K. BUTTERFIELD, North Carolina
DORIS O. MATSUI, California, *Vice Chair*
PETER WELCH, Vermont
KURT SCHRADER, Oregon
TONY CARDENAS, California
ROBIN L. KELLY, Illinois
ANGIE CRAIG, Minnesota
LIZZIE FLETCHER, Texas
FRANK PALLONE, JR., New Jersey *(ex officio)*

ROBERT E. LATTA, Ohio
Ranking Member
STEVE SCALISE, Louisiana
BRETT GUTHRIE, Kentucky
ADAM KINZINGER, Illinois
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
BILLY LONG, Missouri
RICHARD HUDSON, North Carolina
MARKWAYNE MULLIN, Oklahoma
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
JOHN R. CURTIS, Utah
CATHY MCMORRIS RODGERS, Washington
(ex officio)

C O N T E N T S

WITNESSES

SUBMITTED MATERIAL

[1]The legislation has been retained in committee files and is available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=112840.

A SAFE WIRELESS FUTURE: SECURING OUR NETWORKS AND SUPPLY CHAINS

WEDNESDAY, JUNE 30, 2021

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

The subcommittee met, pursuant to call, at 10:30 a.m., in the John D. Dingell Room 2123, Rayburn House Office Building, and remotely via Cisco Webex online video conferencing, Hon. Mike Doyle (chairman of the subcommittee) presiding.

Members present: Representatives Doyle, McNerney, Clarke, Veasey, McEachin, Soto, O'Halleran, Rice, Eshoo, Butterfield, Matsui, Welch, Schrader, Cárdenas, Kelly, Craig, Fletcher, Pallone (ex officio), Latta (subcommittee ranking member), Scalise, Guthrie, Kinzinger, Bilirakis, Johnson, Mullin, Walberg, Duncan, Curtis, and Rodgers (ex officio).

Also present: Representative Joyce.

Staff present: AJ Brown, Counsel; Jennifer Epperson, Counsel; Waverly Gordon, General Counsel; Jessica Grandberry, Staff Assistant; Perry Hamilton, Clerk; Alex Hoehn-Saric, Chief Counsel, Communications and Consumer Protection; Zach Kahan, Deputy Director, Outreach and Member Service; Jerry Leverich, Senior Counsel; Joe Orlando, Policy Analyst; Kaitlyn Peel, Digital Director; Chloe Rodriguez, Clerk; Kate Arey, Minority Content Manager and Digital Assistant; Sarah Burke, Minority Deputy Staff Director; Michael Cameron, Minority Policy Analyst, Consumer Protection and Commerce, Energy, Environment; William Clutterbuck, Minority Staff Assistant/Policy Analyst; Theresa Gambo, Minority Financial and Office Administrator; Jack Heretik, Minority Press Secretary; Nate Hodson, Minority Staff Director; Sean Kelly, Minority Press Secretary; Peter Kielty, Minority General Counsel; Emily King, Minority Member Services Director; Bijan Koohmaraie, Minority Chief Counsel, Oversight and Investigations Chief Counsel; Kate O'Connor, Minority Chief Counsel, Communications and Technology; Clare Paoletta, Minority Policy Analyst, Health; Olivia Shields, Minority Communications Director; Michael Taggart, Minority Policy Director; Evan Viau, Minority Professional Staff Member, Communications and Technology; and Everett Winnick, Minority Director of Information Technology.

Mr. DOYLE. The committee will now come to order.

Today, the Subcommittee on Communications and Technology is holding a hearing entitled "A Safe Wireless Future: Securing Our Networks and Supply Chain."

Due to COVID–19 public health emergency, Members can participate in today's hearing either in person or remotely via online video conferencing. Members who are not vaccinated and participating in person must wear a mask and be socially distanced. Such Members may remove their mask when they are under recognition and speaking from a microphone. Staff and press who are not vaccinated and present in the committee room must wear a mask at all times and be socially distanced.

For Members participating remotely, your microphones will be set on mute for the purpose of eliminating inadvertent background noise. Members participating remotely will need to unmute your microphone each time you wish to speak. Please note that once you unmute your microphone, anything that is said in Webex will be heard over the loud speakers in the committee room and subject to be heard by live stream and C–SPAN.

Since Members are participating from different locations at today's hearing, all recognition of Members, such as for questions, will be in the order of subcommittee seniority.

The Chair now recognizes himself for 5 minutes.

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

I want to thank you all for coming. Thank you to our witnesses, some of whom are here in person and some of whom are here on screens, just as some of our Members are. This is a hybrid hearing, and in a way it highlights the promise of new technologies to our country itself, even as we may resume many in-person activities.

Advances in technology have brought us to this place and allowed us all to continue life as normally as possible over the past year-plus. The pandemic made online work, education, civil engagement, and social interaction a norm and a requirement for large parts of society. Our telecommunication networks and the supply chains that feed those networks answered the increased demand and kept our Nation connected. And while the pandemic is not over yet, it is clear that the need and demand for connectivity will just keep growing.

The bipartisan work of this committee has laid the foundation for the Nation's telecommunications networks to flourish. And to ensure that this continues, we look to foster innovation and competition, protect our networks and supply chains from threats by nontrusted actors, and provide the marketplace with a predictable, stable government, a government that is a partner as well as a regulator.

So let's get to it. There are nine bills before us, a herculean effort, and nearly all of them are bipartisan. We can think of them as loosely falling into three categories.

Three could be considered bills to keep the public, smaller providers, and small businesses educated about how to protect their telecommunications networks and supply chains and to provide support to them as they navigate the changing network and supply chain marketplaces. These are the Understanding Cybersecurity of Mobile Networks Act, the Open RAN Outreach Act, and the American Cybersecurity Literacy Act.

The second group of bills that will unlock—that will lock in support of Government entities to ensure that our networks and supply chains remain safe, these are the Communications Security Advisory Act of 2021, the NTIA Policy and Cybersecurity Coordination Act, among others.

And, finally, the third set of bills will facilitate U.S. leadership with regard to what technologies come next and how we can leverage them to improve the lives of Americans in all corners of our Nation. These are the Secure Equipment Act of 2021, the Information and Communication Technology Strategy Act, and the FUTURE Networks Act.

There is a lot packed into these proposals, and no doubt we will need to make changes to improve and clarify each of them, but I look forward to doing that with my friends and colleagues on both sides of the aisle.

Let me take a moment to discuss the FUTURE Networks Act, which is a bill I introduced along with my friends Representatives McBath and Johnson. The FUTURE Networks Act will require the Federal Communications Commission to create a 6G task force with members appointed by the chair and comprising representatives from trusted companies, public interest groups, and government representatives at every level of government, including Tribes. The mandate of the task force would be to report on possible uses, strengths, and limitations of sixth-generation wireless technology including any supply chain, cybersecurity, or other limitations that will need to be addressed as wireless technology evolves.

Convening a broad group of key stakeholders in the early stages of 6G development will ensure continued U.S. leadership in the global economy. Congress can accelerate our success as a Nation by opening the door to new ideas and inventions and fostering healthy competition here at home.

Our job in this committee is to examine, nurture, and encourage those advances in technology and ensure that they are brought to bear in a manner that makes our lives better. And today's subcommittee hearing, I believe, will help us do just that.

[The prepared statement of Mr. Doyle follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Communications and Technology Chairman Mike Doyle

Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains"

June 30, 2021

Thank you all for coming, and thank you to our witnesses, some of whom are here in person and some of whom are here on our screens, just as some of our members are. This is a hybrid hearing, and, in a way, it highlights the promise of new technologies to our country itself, even as we resume many in-person activities.

Advances in technology have brought us to this place and allowed all of us to continue life as normally as possible over the past year plus. The pandemic made online work, education, civil engagement, and social interaction a norm and a requirement for large parts of our society.

Our telecommunications networks, and the supply chains that feed those networks, answered the increased demand and kept our nation connected. While the pandemic is not yet over, it is clear that the need and demand for connectivity will just keep growing.

The bipartisan work of this committee has laid the foundation for the nation's telecommunications networks to flourish. And to ensure that this continues, we look to foster innovation and competition, protect our networks and supply chains from threats by non-trusted actors, and provide the marketplace with a predictable, stable government—a government that is a partner as well as a regulator.

So let's get to it. There are nine bills before us, a herculean effort and nearly all of them are bipartisan. We can think of them as loosely falling into three categories. Three could be considered bills to keep the public, smaller providers, and small businesses educated about how to protect their telecommunications networks and supply chains, and to provide support to them as they navigate the changing network and supply chain marketplaces. These are the "Understanding Cybersecurity of Mobile Networks Act," the "Open RAN Outreach Act," and the "American Cybersecurity Literacy Act."

The second group are bills that will lock in supportive government entities to ensure that our networks and supply chains remain safe. These are the "Communications Security Advisory Act of 2021" and "the "NTIA Policy and Cybersecurity Coordination Act," among others.

Finally, the third set of bills will facilitate U.S. leadership with regard to what technologies come next and how we leverage them to improve the lives of Americans in all corners of our nation. These are the "Secure Equipment Act of 2021," the "Information and Communication Technology Strategy Act", and the "FUTURE Networks Act."

There's a lot packed into these proposals, and no doubt, we will need to make changes to improve and clarify each of them, but I look forward to doing that with my friends and colleagues on both sides of the aisle.

Let me take a moment to discuss the FUTURE Networks Act, which is a bill that I introduced, along with my friends, Representatives McBath and Johnson. The FUTURE Networks Act would require the Federal Communications Commission to create a 6G Task Force, with members appointed by the Chair, and comprising representatives from trusted companies, public interest groups, and government representatives at every level of government, including tribes. The mandate of the task force would be to report on the possible uses, strengths, and limitations of sixth-generation (6G) wireless technology, including any supply chain, cybersecurity, or other limitations that will need to be addressed as the wireless technology evolves.

Convening a broad group of key stakeholders in the early stages of 6G development will ensure continued U.S. leadership in the global economy. Congress can accelerate our success as a nation by opening the door to new ideas and inventions, and by fostering healthy competition here at home.

Our job in this Committee is to examine, nurture, and encourage those advances in technology and ensure they are brought to bear in a manner that makes our lives better. And today's subcommittee hearing, I believe, will help us do just that.

Mr. DOYLE. I am finished with my opening statement. And it gives me great pleasure now to yield to our ranking member, my good friend Mr. Latta, 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 to my good friend, the chairman of the subcommittee, for holding today's hearing. Greatly appreciate our witnesses being here. It is great to see everybody in person again. It really is. So really great to be here to discuss the nine pieces of legislation which aim to further improve the security of our Nation's communication networks.

Though we don't agree with our Democratic colleagues on every issue, I am proud of our bipartisan record when it comes to securing our communications supply chain. Our leadership in 5G, 6G, and beyond depends on ensuring that all parts of our networks are secure and on having policies that encourage investment in wireless and innovative technologies in the United States.

In April, this committee held a bipartisan hearing on supply chain security issues where there was a bipartisan agreement that we must maintain our global wireless leadership and prevent adversaries like China from threatening our economic national security. Today, I am pleased to see the bipartisan bill before us that would help advance these bills.

As part of this effort, I am working on legislation to require the FCC to develop rules to stipulate the Commission may not certify or authorize any radio frequency devices that originates from the Uyghur autonomous region of the People's Republic of China. This would assist in the effort to help end the forced-labor abuses that have come to light in that region by the Communist—by the Chinese Communist Party.

While this legislation is not being considered today, I hope my colleagues will work with me to advance that legislation going forward.

The bills before us today are just a few important concepts to promote the next generation of secure technologies. We must also acknowledge the advances being made by companies in the United States in these areas.

5G technology opened our eyes to many new vulnerabilities that come with advanced technologies. And as these companies have already begun work on 6G, they are developing innovative solutions to network security. We must ensure that Congress and Federal agencies are up to date on these developments and prepared to knock down any barriers that may arise.

I am pleased that we continue to build on this subcommittee's tradition of bipartisanship on issues of national security, and also thank my friends across the aisle for holding hearings on these bills.

[The prepared statement of Mr. Latta follows:]

Opening Statement of Republican Leader Robert E. Latta
Subcommittee on Communications and Technology
"A Safe Wireless Future: Securing our Networks and Supply Chains"
June 30, 2020

As Prepared for Delivery

Thank you, Chairman Doyle for holding this hearing and to our witnesses for joining us to discuss 9 pieces of legislation which aim to further improve the security of our nation's communications networks.

Though we don't agree with our Democrat colleagues on every issue, I'm proud of our bipartisan record when it comes to securing our communications supply chain. Our leadership in 5G, 6G, and beyond depends on ensuring that all parts of our networks are secure, and on having policies that encourage investment in wireless and innovative technologies in the United States.

In April, this Committee held a bipartisan hearing on supply chain security issues, where there was bipartisan agreement that we must maintain our global wireless

leadership and prevent adversaries like China from threatening our economic and national security. Today, I am pleased to see bipartisan bills before us that would help advance these goals.

As part of this effort, I am working on legislation that would require the FCC to develop rules to stipulate that the Commission may not certify or authorize any radiofrequency device that originates from the Xinjiang Uyghur Autonomous region of the People's Republic of China. This would assist in the effort to help end the forced labor abuses that have come to light in that region by the Chinese Communist Party. While this legislation is not being considered today, I hope my colleagues will work with me to advance that legislation going forward.

The bills before us today are just a few important concepts to promote the next generation of secure technologies. We must also acknowledge the advancements being made by companies in the United States in these areas. 5G technology opened our eyes to many new vulnerabilities that come with advanced technologies, and as these companies have already begun

work on 6G, they are developing innovative solutions to network security. We must ensure that Congress and federal agencies are up to date on these developments and prepared to knock down any barriers that may arise.

I am pleased that we are continuing to build on this subcommittee's tradition of bipartisanship on issues of national security and thank my friends across the aisle for holding a hearing on these bills.

I will now yield the remainder of my time to my colleague from Ohio, Mr. Johnson.

I look forward to hearing feedback from our esteemed witness panel and continuing to work together to pass substantive, bipartisan policies to maintain our strength and leadership in wireless innovation.

Mr. LATTA. Mr. Chairman, at this time, I would now yield the balance of my time to my good friend and colleague, the gentleman from Ohio, Mr. Johnson.

Mr. JOHNSON. Well, I thank the ranking member for yielding.

I am very pleased that my bill, H.R. 4029, the TEAM TELECOM Act, is included in today's legislative hearing. This legislation is very straightforward. It simply codifies the existing executive branch process for performing national security reviews when requests are submitted to the FCC for provider services and when an applicant exceeds the foreign ownership threshold.

This process includes an interagency working group composed of national security and law enforcement representatives that provide the FCC with the recommendation to either fully grant, grant conditionally on mitigation, or deny the application based on their national security or law enforcement perspective. It is critically important that we equip the FCC with the tools necessary to protect America's telecommunications networks from foreign interference or manipulation.

H.R. 4029 provides certainty and transparency to the TEAM TELECOM review process that would protect our national security interests, while providing foreign investors a straightforward application process that includes standardized application questions and a timely review and notification process. Having NTIA in charge of the coordinating efforts would also build on their interagency coordination role while preserving the subject matter expertise of appropriate national security and intelligence agencies that compose TEAM TELECOM.

And, finally, I welcome any of my colleagues on the Democratic side to join me as a cosponsor of this very commonsense legislation.

Thank you again for yielding, and I yield back.

Mr. LATTA. Well, I thank the gentleman.

And, Mr. Chairman, I look forward to hearing the feedback from our esteemed witness panel, and continue to work together to pass substantive bipartisan policies to maintain our strength and leadership in wireless innovation within the industry.

And I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair now recognizes Mr. McNerney for 5 minutes for his opening statement.

OPENING STATEMENT OF HON. JERRY MCNERNEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. MCNERNEY. Well, I thank the chairman. I am glad we are having this hearing today because, as we have watched wireless communication technologies and networks evolve, I am concerned that our security technologies may not be keeping pace. Consumer demand is driving the growth of wireless devices that connect to the internet, while this country simultaneously faces increasing threats to our networks and supply chains. Moreover, Internet of Things devices can be hijacked by bad actors, including foreign adversaries, to target other parts of the network infrastructure, and wireless networks can also be exposed to risks by their own network components.

The risk has grown as foreign, nontrusted companies have become major providers in the telecommunication supply chain both here and around the world. Addressing risks to our own supply chain will take more than just industry or just government to solve. Congressional action is needed to help the industry fortify itself.

Today, we are considering a fair number of bills, and I have cosponsored almost all of them. Each bill does something different, but they all have a similar aim, which is to strengthen the Nation, its consumers, and trusted companies we partner with against network and supply chain risks.

First, I am coleading, along with Representatives Long and Spanberger, H.R. 4028, the Information and Communication Technology Strategy Act, which would direct the Secretary of Commerce to report on economic competitiveness of trusted vendors in the information and communications technology supply chain, identify which components or technologies are critical or vulnerable, and identify which components or technologies the U.S. networks cannot work without.

Next, I am cosponsoring H.R. 3919, the Secure Equipment Act of 2021, with Representatives Eshoo and Scalise. This bill would provide the FCC—would prohibit the FCC from reviewing or approving applications from companies on the Commission's covered list as required under the Secure and Trusted Communications Network Act.

There are several other bills, all thoughtful products of my colleagues on both sides of the aisle, and I look forward to hearing more about them today.

Representative Doyle's FUTURE Network Act will ensure that we stay on top of policy considerations as wireless services continue to evolve. Representative O'Halleran's Open RAN Outreach bill will help smaller providers stay competitive in the U.S. market by helping them consider their network options. Representative Kinzinger's Cybersecurity Literacy Act will empower families and businesses with information to keep their digital lives secure. And Representative Schrader's Communication Security Advisory Act will institutionalize an important public and private forum for sharing information and best practices.

I will let the other cosponsors talk about the bills, but in general the reason why I am cosponsoring these bills is because, in one way or another, each one either supports our consumers and smaller providers by educating them about risks and threats, while also encouraging competition and innovation, or pushes the country forward by fostering network security thought leadership with our agencies performing a much-needed steady hand at the wheel. These are important initiatives and will help our country enter the age, not just the 5G, but of 6G and beyond, and do it safely and securely.

Thank you, Mr. Chairman. And I yield back.

[The prepared statement of Mr. McNerney follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Member Rep. Jerry McNerney

Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains"

June 30, 2021

I am glad we are having this hearing today, because, as I have watched the wireless communications technologies and networks evolve, I have also felt concerned that our security technologies may not keep pace. Consumer demand, especially now, is driving the growth of wireless devices that can connect to the internet while this country simultaneously faces increasing threats to our networks and supply chains. Vulnerable internet of things devices can be highjacked by bad actors, including foreign adversaries, to target other parts of the network infrastructure, and wireless networks can also be exposed to risk by their own network components.

The risk has grown as we have watched foreign non-trusted companies become major provider in the telecommunications supply chain, both here and around the world. Addressing risks to our supply chains will take more than just industry or just government action to solve. Congress can and should help the industry fortify itself.

Today, we are considering a fair number of bills, and I have co-sponsored almost all of them. Each bill does something different, but they all have a similar aim, which is to gird the nation, its consumers, and the trusted companies we partner with against network and supply chain risk.

First, I am co-leading, along with Representatives Long and Spanberger, H.R. 4028, Information and Communication Technology Strategy Act, which would direct the Secretary of Commerce to report on the economic competitiveness of trusted vendors in the information and communication technology supply chain, identify which components or technologies are critical or vulnerable, and identify which components or technologies U.S. networks can't work without.

Next, I am co-sponsoring H.R. 3919, the Secure Equipment Act of 2021, with Representatives Eshoo and Scalise. The bill would prohibit the FCC from reviewing or approving applications from companies on the Commission's "Covered List," as required under the Secure and Trusted Communications Networks Act.

There are several other bills, all the products of the thoughtfulness of my colleagues on both sides of the aisle, that I look forward to hearing about today. Representative Doyle's FUTURE Networks Act will ensure that we stay on top of the policy considerations as wireless services continue to evolve. Representative O'Halleran's Open RAN Outreach bill will help smaller providers stay competitive in the U.S. market by helping them consider their network options. Representative Kinzinger's Cybersecurity Literacy Act will empower families and

business with information to help keep their digital lives secure. And Representative Schrader's Communications Security Advisory Act will institutionalize an important public-private forum for sharing information and best practices.

I'll let the other sponsors talk about these bills, but in general the reason why I am co-sponsoring these bills is because in one way or another each one either supports our consumers and smaller providers by educating them about risks and threats while also encouraging competition and innovation or pushes the country forward by fostering network security thought-leadership with our agencies performing as a much-needed steady hand at the wheel.

These are important initiatives and will help the country enter the age, not just of 5G, but of 6G and beyond, and do it safely and securely. Thank you and I yield back.

Mr. DOYLE. The Chair recognizes Mrs. Rodgers, the ranking member of the full committee, for 5 minutes for her opening statement.

OPENING STATEMENT OF HON. CATHY MCMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mrs. RODGERS. Thank you, Mr. Chairman.

Welcome, everyone.

With the recent cyber attacks on our critical infrastructure and priorities to secure America's competitive edge from adversaries like China and Russia, it is crucial that we continue to bolster our economic success and global leadership. We do not want the Chinese Communist Party setting standards for 5G and 6G. America must be at the forefront. It is our duty to find solutions to ensure a robust and secure supply chain for our communications networks.

Today, I am pleased that we are considering bipartisan legislation that builds on our past achievements to advance our economic and national security. We worked together to pass the Secure and Trusted Communications Networks Act and because we all agree that we need to stop our adversaries from placing their equipment on our networks.

For communication networks, we have also taken concrete actions to facilitate and support the next wave of innovation, including open RAN technology to increase vendor diversity and strengthen American and allied companies. Now we must work together to strengthen our security of our networks as the industry deploys advanced technologies.

We have a slate of important legislation we are discussing today, including H.R. 4028, Mr. Long's ICT Strategy Act, which will direct NTIA to identify which components or technologies are crucial and possibly vulnerable in networks in the United States. NTIA would use this information to develop a whole-of-government strategy to ensure the economic competitiveness of trusted communication technology vendors. It is critical that we push back against Huawei and others who are undercutting the trusted supply chain.

I will now yield to my colleague, Mr. Duncan, to talk about his bipartisan bill.

Mr. DUNCAN. I thank the ranking member.

And I first want to thank Chairman Doyle for your efforts to bring bipartisan legislation forward. Your efforts are noted and appreciated.

I want to speak in support of our bipartisan legislation, H.R. 4046, the NTIA Policy and Cybersecurity Coordination Act. Everyone knows our Nation has been under constant attack from cyber criminals, including state sponsors and multinational criminal cartels, who have used ransomware attacks against pipelines, hospitals, schools, local governments, and businesses of every shape and size. We must coordinate our policy responses across Federal Government to protect our people in a coordinated way.

So our bill will allow the NTIA to build on their multistakeholder policy development and expertise to act as a central clearinghouse for cybersecurity policy development to respond to and prevent these attacks from succeeding. This bill codifies the existing Office

of Policy Analysis and Development and allows them to continue current functions. We then rebrand the office to elevate the cybersecurity focus and expand the cybersecurity policy development role of that office to play a coordinating function all across Federal Government.

So I want to also thank my original cosponsors, Susan Wild of Pennsylvania and John Curtis of Utah, for their bipartisan support. And I ask the whole committee to support this important legislation.

I yield back the balance of my time.

Mrs. RODGERS. Mr. Chairman, I will just say thank you again for today's hearing. Appreciate you bringing forward these bipartisan bills on an important subject, and look forward to hearing from our witnesses.

I yield back the balance of my time.

[The prepared statement of Mrs. Rodgers follows:]

Opening Statement of Republican Leader Cathy McMorris Rodgers
Subcommittee on Communications and Technology
"A Safe Wireless Future: Securing our Networks and Supply Chains."
June 30, 2021

As Prepared for Delivery

Good morning and thank you, Mr. Chairman.

With recent cyberattacks on our critical infrastructure and priorities to secure America's competitive edge from adversaries like Russia and China…

... it's crucial we continue to bolster our economic success and global leadership.

We do not want the Chinese Communist Party setting the standards for 5G and 6G.

America must be at the forefront…

It's our duty to find solutions that ensure a robust and secure supply chain for our communications networks.

Today, I am pleased that we are considering bipartisan legislation that builds on our past achievements to advance our economic and national security.

We worked together to pass the Secure and Trusted Communications Networks Act…

... because we all agree that we need to stop our adversaries from placing their equipment in our networks.

For communication networks, we've also taken concrete actions to facilitate and support the next wave of innovation, including Open-RAN technology, to increase vendor diversity and strengthen American and allied companies.

Now, we must work together to strengthen the security of our networks as industry deploys advanced technologies.

We have a slate of important legislation we are discussing today, including H.R. 4028, Mr. Long's ICT Strategy Act…

…which would direct NTIA to identify which components or technologies are critical, and possibly vulnerable, in networks in the United States.

NTIA would use this information to develop a whole of government strategy to ensure the economic competitiveness of trusted communications technology vendors.

It is critical that we push back against Huawei and others who are undercutting the trusted supply chain.

I will now yield one minute to my colleague Mr. Duncan to talk about his bipartisan bill.

[Yield to Mr. Duncan].

I look forward to working together with all of my colleagues on this committee to advance these important pieces of legislation.

I yield back.

Mr. DOYLE. I thank the gentlelady. The gentlelady 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 it is now my great pleasure to introduce our witnesses for today's hearing.

Mr. Dileep Srihari, senior policy counsel, Access Partnership. Welcome.

Mr. Jason Boswell, head of security, Network Product Solutions, Ericsson. Welcome.

Mr. Dean Brenner, SVP, senior vice president, spectrum strategy and tech policy, Qualcomm Incorporated. Welcome.

And last but certainly not least, Mr. Clete Johnson—I love that first name, Clete Johnson; there must have been a baseball player in your family—senior fellow, Strategic Technologies Program, Center for Strategic and International Studies.

We want to thank our witnesses for joining us. We look forward to your testimony.

The Chair is going to recognize each witness for 5 minutes. Now, if you go over 5 minutes, a trap door opens beneath your chair and you will never be heard from again. This subcommittee has—this particular subcommittee are sticklers for not only our witnesses but especially our Members on both sides of the aisle adhering to the 5-minute rule and not to ask questions with 3 seconds left that causes the witness to talk 2 more minutes. So, with those admonitions, we will get started.

And we will recognize Mr. Srihari for 5 minutes.

STATEMENTS OF DILEEP SRIHARI, SENIOR POLICY COUNSEL, ACCESS PARTNERSHIP; JASON BOSWELL, HEAD OF SECURITY, NETWORK PRODUCT SOLUTIONS, ERICSSON NORTH AMERICA; DEAN R. BRENNER, SENIOR VICE PRESIDENT, SPECTRUM STRATEGY AND TECH POLICY, QUALCOMM INCORPORATED; AND CLETE D. JOHNSON, SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

STATEMENT OF DILEEP SRIHARI

Mr. SRIHARI. Thank you, Mr. Chairman.

Chairman Doyle, Ranking Member Latta, members of the subcommittee, my name is Dileep Srihari, and I am senior policy counsel at Access Partnership, a global tech policy consulting firm. Thank you very much for the opportunity to appear before you today in person. I am very honored to be here today.

My statement this morning will focus on three general topic areas: first, the promise of open network architectures, including open RAN; second, maintaining and promoting U.S. technological leadership; and third, ensuring that NTIA and the FCC are well positioned to meet heightened expectations regarding network supply chain security.

First, on open networks, open networks enable the disaggregation of traditional network infrastructure elements, such as the base station in a radio access network, or RAN, into subelements and functions. This enables interoperability between products and vendors and thus increases competition.

The global RAN infrastructure market has been dominated by a handful of companies, but the move towards open RAN is unlocking the market and enabling new entrants, especially American companies who lead in software.

To keep things moving, Congress should do several things. First, fund the USA TELECOM Act. The House should provide at least $1.5 billion for the USA Telecom domestic fund, $500 million for the multilateral fund, consistent with the Senate's approach.

Second, support both the public and private sector test beds to help build greater confidence among U.S. operators, even as the technology is already being deployed today.

Third, provide support for companies, especially small companies, to participate in relevant standards organizations.

Fourth, promote outreach and education for smaller and rural operators, building on the open RAN showcase that Acting Chairman Rosenworcel is hosting in 2 weeks.

Finally, Congress as a whole should streamline access to funding for U.S. open RAN vendors competing for business overseas. The competition is fierce, and some of the foreign vendors benefit from mass subsidies and other noncompetitive advantages.

A second topic is maintaining U.S. leadership in next-generation technology. One of the best ways to strengthen the supply chains of U.S. networks is to ensure that the domestic ICT industry continues to lead the world.

On 6G, the EU is supporting a consortium whose explicit purpose is to put Europe at the forefront of research and development in 6G. There is also little doubt that China intends to seek leadership in this space.

Industry should ultimately be leading the way towards new standards, but early strategic partnerships could potentially prove beneficial.

Congress should also begin regularly reinvesting a portion of spectrum auction revenue into telecom purposes. Since the 2012 Spectrum Act was enacted, the Federal Government has collected over $150 billion in gross proceeds from spectrum auctions. While it may be tough to look backward, Congress should plan ahead now for future reinvestment. Some have proposed a 10 percent rural dividend from spectrum auctions—it should be higher—but we also need a research dividend. Even 1 percent of auction proceeds over the past decade, which works out to roughly $1.5 billion, would have been significant, although we should now aim higher.

Finally, my third topic is that this subcommittee needs to ensure that NTIA and the FCC are well organized and capable of carrying out their assignments in these areas. Six of the nine bills before you today would potentially add to or reconfigure NTIA's workload. The members of this subcommittee must ensure that NTIA has the capacity to execute on these additional functions.

As I have explained in my written statement, the relevant staffing within NTIA is actually quite small, although the President is currently proposing some increases.

Finally, this hearing illustrates that NTIA needs an Administrator, given the growing importance of what it is being asked to do. Ideally, Congress should hear from NTIA itself on these issues, and the Administrator position was vacant during the previous ad-

ministration for far too long. You should urge the President to fill this vacancy.

Mr. Chairman, thank you again for the opportunity to appear before you this morning. I look forward to answering your questions.

[The prepared statement of Mr. Srihari follows:]

Dileep Srihari
Senior Policy Counsel, Access Partnership

"A Safe Wireless Future: Securing Our Networks and Supply Chains"
Subcommittee on Communications and Technology
House Committee on Energy and Commerce
June 30, 2021

Chairman Doyle, Ranking Member Latta, and Members of the Subcommittee:

My name is Dileep Srihari and I am Senior Policy Counsel at Access Partnership, a global technology policy consulting firm. My work focuses on data policy, cybersecurity, and telecommunications infrastructure issues, including diversification and security of the information & communications technology (ICT) supply chain. Thank you very much for the opportunity to appear before you. I am honored to be here today.

My statement will focus on three broad topic areas:

- *First*, the promise of open network architectures including Open RAN, along with concrete steps Congress should take to promote the growth of that ecosystem;
- *Second*, maintaining and promoting U.S. technological leadership in the global communications space; and
- *Third*, ensuring that NTIA and the FCC are well-positioned to meet heightened expectations.

I. Promoting Open Network Architectures

Where Things Stand

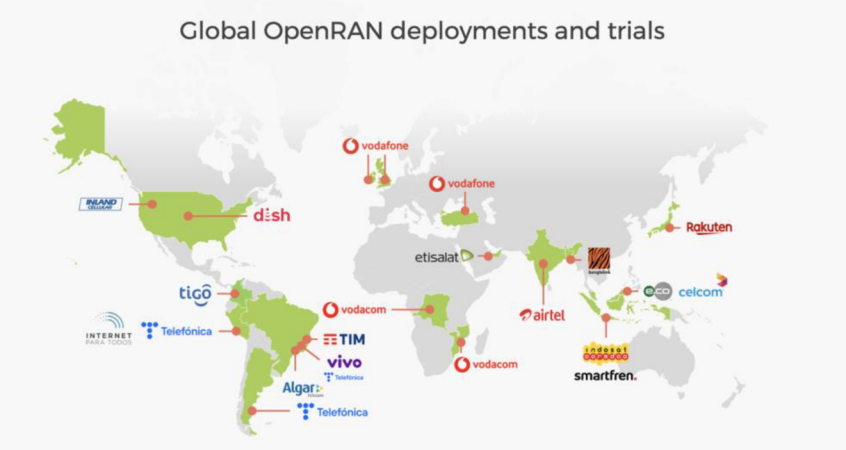
Open network architectures enable the disaggregation of traditional network infrastructure elements – such as the *base station* in a radio access network (RAN) – into sub-elements and functions. A system of standardized interfaces allows the various sub-elements to communicate with each other, enabling interoperability between products and vendors and thus increased competition. Open architectures also allow network functions that were previously implemented through dedicated or customized hardware to be implemented through software instead, with the software running on more general-purpose hardware.

While the global RAN infrastructure market has recently been dominated by a handful of companies, the move toward Open RAN is unlocking the market and enabling new entrants, including both large and small American companies. In particular, the move from customized hardware to software is also leveraging the competitive global advantage of the United States in the software space. This virtualization of network functions also allows operators to move some

functions away from the edge of their networks closer to the core – or vice-versa – unleashing the potential of cloud-based network infrastructure and ultra-low-latency networking.

All of this brings numerous benefits for operators and, in turn, consumers. To begin with, open and disaggregated architectures provide operators with increased flexibility, avoiding the problem of "vendor lock-in." Open architectures also reduce the cost of infrastructure deployments: for example, Japanese company Rakuten has cited savings of 40% in capital expenditures (CAPEX) and 30% in operational expenditures (OPEX) through their adoption of an Open RAN solution.[1] The movement toward software and cloud-based architecture also leads to technological benefits based upon artificial intelligence and machine learning, including automated threat detection and mitigation. Finally, by enabling more companies to compete based on security, open network architectures will ultimately increase network security.

Open RAN deployments are moving forward rapidly in both urban and rural environments around the world. As shown below, most trials and early deployments at this moment are happening outside the United States:



Source: Telecom Infra Project[2]

[1] Comments of Rakuten Mobile USA, LLC, filed Apr. 28, 2021 in FCC GN Docket No. 21-63, at 5-6, https://ecfsapi.fcc.gov/file/104290618324318/Rakuten%20Comments.pdf.

[2] Telecom Infra Project, *TIP's OpenRAN Project Group Accelerates the Development, Validation, and Deployment of OpenRAN Solutions*, June 24, 2021, https://telecominfraproject.com/openran-project-group-accelerates-development-validation-deployment-openran-solutions/.

However, most of these overseas deployments have involved American *vendors* supplying the Open RAN technology to the foreign operator, providing either a software solution or a complete systems integration. Meanwhile, DISH plans to deploy a nationwide network in the United States based on Open RAN, and other U.S. carriers are making plans or have already started to deploy the technology.

Next Steps

Congress should continue taking steps to encourage the adoption of Open RAN and other open network architectures more widely, both at home and abroad. Specific steps for consideration should include:

Funding the USA TELECOM Act. The USA TELECOM Act, enacted last year as part of the FY21 NDAA, authorized an NTIA-administered grant program to promote open network technology. It also authorized a multilateral telecommunications security fund. However, Congress has not yet enacted appropriations for either fund.

- The United States Innovation and Competition Act (USICA, S. 1260), recently passed by the Senate, would appropriate $1.5 billion for the NTIA grant program. It would also appropriate $500 million for the multilateral program, along with a multilateral effort on semiconductors. As the House considers its response to the Senate bill, this Subcommittee should strongly push for the funding to be included. Federal investment in Open RAN and other open network architectures is critical to establishing the technology, and would complement efforts by governments in Germany, the United Kingdom, and elsewhere.

Supporting Testbeds and Participation in Standards-Setting. Section 2520(a) of USICA would authorize a testbed for open network architectures at NTIA's Institute for Telecommunications Sciences in Boulder, CO. In addition, Section 2520(b) would create a grant program for smaller companies to participate in global standards-setting organizations, especially companies who would not otherwise be able to participate without the grant. The House should support these provisions, and also ensure that funding will be made available for private-sector testbeds and other testing and validation activities as well.

Operator Education and Outreach. Even within the United States, awareness of Open RAN and other open network architectures remains limited – especially among small and rural operators. The federal government has an important role to play in conducting outreach, and Acting Chairwoman Rosenworcel has taken the lead by planning an "Open RAN Showcase" for operators that will be held on July 14-15, 2021.[3]

[3] FCC, *Open RAN Solutions Showcase – Day 1*, https://www.fcc.gov/news-events/events/2021/07/open-ran-solutions-showcase-day-1 (visited June 28, 2021).

- The **Open RAN Outreach Act (H.R. 4032)** would require NTIA to conduct outreach and provide technical assistance to small communications network providers to raise awareness. Meanwhile, Section 8 of the Secure and Trusted Communications Networks Act of 2019 created the C-SCRIP program by which NTIA is conducting outreach to smaller operators on supply chain security risks.[4] There may be potential opportunities for synergy between the C-SCRIP program and outreach on Open RAN.

- Thoughtfully, the bill's definition of "open network architecture" includes not just Open RAN, but also open core and open transport as well. This is consistent with the approach taken in Section 2520 of USICA. While Open RAN often receives more attention, the movement toward open and disaggregated network architectures is a broader one that includes all elements of end-to-end connectivity from the edge to the core.

Streamlining Access to Funding for Overseas Projects. American ICT vendors continue to face significant headwinds in winning business from telecom operators around the world, especially in developing countries. In many cases, local operators and governments are unaware of Open RAN, requiring significant effort by the vendors to fill the knowledge gap. Meanwhile, incumbent vendors leverage their established relationships – and in some cases, large subsidies from their home countries – to capture the market and raise the barrier for new entrants and new technologies.

The federal government has taken some helpful steps in recent years, including the reauthorization of the U.S. Export-Import Bank in late 2019. However, U.S. Open RAN vendors still encounter difficulties in obtaining the financing necessary to compete with other vendors when responding to operators' requests for proposals (RFPs). Congress should therefore consider further steps in this area. For example, agencies such as EXIM or the U.S. Trade and Development Agency (USTDA) should consider guaranteeing funding in advance to *any* U.S. company that may win a particular RFP, thus strengthening the competitiveness of American proposals. USAID can also play an enhanced role, either in directly promoting development or by supporting education and outreach efforts around the world.

II. Maintaining U.S. Leadership in Next-Generation ICT

It has been said that "the best defense is a great offense." In the context of today's hearing, one of the best methods to strengthen the supply chains underlying U.S. networks is to ensure that the domestic ICT industry continues to lead the way in global technology development.

Looking Ahead to 6G. It is not too soon for the United States to begin looking forward to the next generation of wireless technology, not least because of what is happening elsewhere. In

[4] NTIA, *C-SCRIP*, https://www.ntia.doc.gov/cscrip (visited June 28, 2021); Secure and Trusted Communications Networks Act of 2019 § 8, Pub. L. No. 116-124, 134 Stat. 158, 168, https://www.congress.gov/116/plaws/publ124/PLAW-116publ124.pdf.

Europe, the Hexa-X consortium project has been sponsored by the European Union, and describes its purpose as being a "flagship action capable [of putting the] EU at the forefront of research and development in [6G]."[5] The project has received funding from the EU's Horizon 2020 research and innovation program. Meanwhile, China announced plans in 2019 to launch a nationally coordinated R&D effort focused on 6G, and while this was reasonably regarded as being hyperbole at the time, there is little doubt that China intends to seek leadership in this space.[6]

- The **FUTURE Networks Act (H.R. 4045)** would establish a 6G Task Force under the auspices of the FCC to begin developing an American effort in this area. While industry should ultimately lead the way toward standardization of next-generation technologies, bringing together various stakeholders from industry, government, and elsewhere at an early stage of development should prove beneficial.

Re-Investing Spectrum Auction Proceeds in R&D. In the decade since the 2012 Spectrum Act was enacted,[7] the federal government has collected over $150 *billion* in gross proceeds from spectrum auctions.[8] If even *half* of this amount had been re-invested into the telecommunications ecosystem, the United States would potentially have achieved universal broadband access by now, and the U.S. ICT industry's posture would likely have been much stronger in comparison to global competitors.

While it may be difficult or impossible to redirect proceeds from prior auctions, Congress should learn the lessons of the past and act now to ensure that a significant portion of *future* auction proceeds are reinvested into the ICT ecosystem. Some have proposed a ten-percent "rural dividend" from spectrum auctions, but Congress should also establish a "research dividend" as well. Even *one* percent of auction proceeds over the past decade – roughly $1.5 billion – would have represented a significant federal investment into wireless R&D.

---

[5] Hexa-X, Hexa-X Consortium, https://hexa-x.eu/consortium/ (visited June 27, 2021).

[6] Brandi Vincent, *China Said It's Developing 6G. What Does That Mean?*, Nextgov, Nov. 11, 2019, https://www.nextgov.com/emerging-tech/2019/11/china-said-its-developing-6g-what-does-mean/161225/.

[7] Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, title VI (commonly referred to by the FCC as the "Spectrum Act").

[8] FCC, *Auctions Summary*, https://www.fcc.gov/auctions-summary (visited June 27, 2021). Notable auctions include the 2015 AWS-3 auction ($41.3 billion), the 2017 broadcast incentive auction ($19.3 billion), and the 2021 C-Band auction ($81.1 billion).

III. Aligning Federal Agencies to Meet the Challenge

Several of the bills under consideration in today's hearing would take steps to better align or prepare NTIA and the FCC to meet the challenge. For example:

- The **TEAM TELECOM Act (H.R. 4029)** would codify the Team Telecom process. Codification makes sense given the consequential role that Team Telecom has been playing in recent years, while also bringing a measure of transparency to the process including some procedural safeguards.

- The **Communications Security Advisory Act of 2021 (H.R. 4067)** would codify the FCC's Communications, Safety, Reliability, and Interoperability Council (CSRIC). Codification would elevate the importance of the body and build on the recent announcement from Acting Chairwoman Rosenworcel that she wants the CSRIC to consider supply chain security matters in earnest.[9]

- The **NTIA Policy and Cybersecurity Coordination Act (H.R. 4046)** would recognize the increasingly important role that NTIA is playing in ICT supply chain security. The bill would reconfigure the Office of Policy Analysis and Development (OPAD) into the Office of Policy Development and Cybersecurity. Some of the other measures being considered today would likely be implemented by that office.

Re-Investing in NTIA. Five of the nine bills being considered today would potentially add to, or reconfigure, NTIA's workload. A sixth would require work by the Department of Commerce as a whole, of which a significant part would be handled by NTIA. As Congress increases its expectations of NTIA, it should ensure that the agency's resources continue to increase concomitantly. For example, while conducting operator outreach on Open RAN and conducting a national cybersecurity literacy program are both important undertakings, this Subcommittee must ensure that the agency's staff has the capacity to execute them.

- Many or most of the activities in the bills being considered today would fall under NTIA's umbrella "Domestic and International Policies" budget category.[10] The staffing for this function is quite small, with only 27 staff positions as recently as FY2020.[11] This was increased to 39 positions in FY2021 and the President is proposing an increase to 52 positions in FY22 in order to implement Executive Order 13873 on Securing the ICTS

---

[9] FCC Public Notice, *FCC Acting Chairwoman Announces Advisory Committee Will Focus on 5G Network Security and Software Vulnerabilities*, Apr. 15, 2021, https://docs.fcc.gov/public/attachments/DOC-371641A1.pdf.

[10] NTIA, *FY 2022 Budget as Presented to Congress*, May 2021, at 25-28, https://www.commerce.gov/sites/default/files/2021-05/fy2022_ntia_congressional_budget_justification.pdf.

[11] *Id.* at 17.

Supply Chain.[12] As the agency's duties continue to increase, this Subcommittee should strongly support further efforts to increase NTIA staffing.

Confirming an NTIA Administrator. The lack of a confirmed NTIA Administrator is increasingly problematic given the growing importance of the functions that Congress expects the agency to carry out. For various reasons, the position was vacant during the previous Administration for much too long. Congress should urge the current Administration to act promptly to fill the vacancy.

IV. Cybersecurity Education

Finally, the **American Cybersecurity Literacy Act (H.R. 4055)** is also under consideration today. Although not focused primarily on network infrastructure supply chains, a federal government campaign to educate the public could potentially help prevent many security breaches.

While estimates vary, it is widely accepted that a large fraction of successful cybersecurity attacks result from poor "cyber hygiene" – such as weak passwords or basic user error – rather than sophisticated technical attacks. A better understanding of basic cyber hygiene principles among a larger fraction of the American public could potentially reduce the collective impact of data breaches on individuals, businesses, and governments alike.

****

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

[12] *Id.* at 29.

Mr. DOYLE. And I would note that he left 50 seconds on the clock.

Mr. Boswell, you are recognized for 5 minutes.

STATEMENT OF JASON BOSWELL

Mr. BOSWELL. Thank you.

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers——

Mr. DOYLE. Would you check if your microphone is on?

Mr. BOSWELL. It says—it is red. Can you not hear me? Could it be a little bit closer?

Mr. DOYLE. Pull it a little closer to you.

Mr. BOSWELL. Let's try that. Is that better? OK. Shall I start over, please? OK. I will let the time—there we go.

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers, members of the committee, thank you for the opportunity to share Ericsson's views on secure and reliable wireless communications. We appreciate your ongoing focus on secure communications networks, which are a top priority for me, for Ericsson, and for our Nation.

Ericsson has focused on network security for decades, contributing to numerous technical committees and standards bodies and establishing dedicated internal security organizations. As head of security for Network Product Solutions in Ericsson North America, I represent Ericsson in collaborative government efforts, including President Biden's NSTAC, the FCC's CSRIC, the DHS ICT Supply Chain Risk Management Task Force, and on the executive committee of the Communications Sector Coordinating Council, as well as many other initiatives.

Since I last testified before Congress on March 4, 2020, our society has learned the indispensable value of secure, reliable, remote connectivity in every aspect of our lives. I know from my work at Ericsson and from my service on the NSTAC and on other bodies that the telecommunications industry as a whole has stepped up and excelled during this historic challenge. We are in a pivotal moment for the future of secure, reliable wireless communications, and we must not lose focus.

5G will accelerate innovation and deliver transformative benefits and will be the most secure network generation yet. And at this moment, we have an opportunity for the U.S. to set a global example across policy, technology, and standards.

I want to share Ericsson's perspective on key priorities and action items which can help guide us.

Ericsson serves customers in the U.S. and in more than 180 other countries, with nearly 8,000 U.S. employees. While our global headquarters is in Sweden, a longtime U.S. partner and defense treaty ally, the U.S. is effectively our domestic market as it is our largest market and it drives our global R&D investments.

We have key operations here and maintain strategic partnerships with many U.S. companies, such as Qualcomm, NVIDIA, Intel, and Juniper. In fact, the vast majority of all active intelligent electronics for our radio systems and even the silicon itself, which comes from Intel fabs, are sourced from U.S. companies.

We are actively expanding our investment in U.S. manufacturing and jobs, opening a $100 million 5G smart factory in Texas last year and maintaining four U.S. R&D locations. We were also the first vendor to launch 5G across the U.S. We are committed to helping close the digital divide in rural America.

Ericsson recognizes that security is fundamental to the success of 5G networks and commits significant resources to ensure that networks are trustworthy, resilient, and secure by design. Across all of our facilities, Ericsson secures our own supply chain with tight quality controls, traceability, integrity checks, site audits, tests and verifications. And years before the disruptions caused by COVID–19, we initiated a regionalization strategy for our supply chain to mitigate potential risks or regional disruptions—excuse me—and reduce our dependence on one supply site or vendor. Well before the attack on SolarWinds last year, all of Ericsson's software was subject to rigorous software development practices.

The subcommittee can support our common goals of ensuring that U.S. telecommunications networks stay safe and secure in the following ways.

First, pass, implement, and oversee legislation to promote wireless security. We commend you for developing and engaging with industry on the proposed legislation under discussion today, and we look forward to working with you on these bills and in future hearings such as this.

Second, support actions to accelerate 5G deployment through increased spectrum access, streamlined small cell siting rulings, and incentives for rural build-out, and by ensuring wireless and 5G infrastructure qualify for funding in any broadband infrastructure funding legislation.

Third, continue to enable a secure and robust marketplace of trusted suppliers. It is critical to leverage strategic codependencies among the U.S. and its partners and allies and develop policies that foster a diverse, trusted global market of suppliers that deliver high-performing, secure, and energy-efficient network products to U.S. operators.

Finally, continue to maintain a policy of technology neutrality. Ericsson heartily supports openness and the evolution toward open architectures, and that shift is taking place today within Ericsson and the industry without any government mandates or preferences.

On behalf of Ericsson, I thank the subcommittee for its leadership in this area. I look forward to the work ahead, and I welcome your questions.

[The prepared statement of Mr. Boswell follows:]

Testimony of Jason Boswell
Head of Security
Network Product Solutions
Ericsson North America

on
"A Safe Wireless Future:
Securing our Networks and Supply Chains"

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

June 30, 2021

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers, Members of the Committee, thank you for the opportunity to appear today to share Ericsson's views on the future of secure and reliable wireless communications. We appreciate your ongoing focus on secure communications networks—a matter of top priority to Ericsson and of critical importance to our nation.

Ericsson has focused on network security for decades, contributing to numerous technical committees and standards bodies, and establishing dedicated internal security organizations. As Head of Security for Network Product Solutions in Ericsson North America, I advise Ericsson's technicians, engineers, partners, and customers on secure Ericsson solutions. I also represent Ericsson in numerous industry initiatives and collaborative efforts with government, including the President's National Security Telecommunications Advisory Committee (NSTAC) and the Network Security Information Exchange (NSIE), on the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC), on the Department of Homeland Security's (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, as well as many other working groups and committees.

The last time I had the honor to testify before Congress was March 4, 2020, and in the ensuing 15 months, our society has learned the indispensable value of secure, reliable, remote connectivity in virtually every aspect of our lives, from education to business to social activities. I know from my work at Ericsson – and from my service on NSTAC and other bodies – that the ICT industry as a whole has stepped up and excelled during this historic challenge.

The ICT industry is using a model of private sector leadership facilitated by coordinated government partnership. As part of NSTAC, during the past year I co-authored two reports to the President on (1) ICT resiliency during COVID-19 and recommended steps that the Administration should take to ensure the resiliency of U.S. national security and emergency preparedness (NS/EP) communications and (2) a long-term look-ahead to communications security and reliability demands of the future. In these reports, and in other collaborative efforts, experts across the ICT industry have coalesced around three core goals to protecting the nation's critical infrastructure:

1. Secure the communication itself, end to end;
2. Ensure the resilience of the network; and
3. Protect the integrity of the network supply chain.

These pillars are important whether we're talking about 3G, 4G, 5G, Wi-Fi, cloud environments, or wireline infrastructure. The thoughts I share with you today derive from this work.

Above all else, I want to emphasize that we are in a pivotal moment for the future of secure, reliable wireless communications. We must not lose focus.

5G will accelerate innovation and deliver transformative benefits by enabling greater connectivity, lower latency, enhanced capacity, and more sophisticated network management. While this increased connectivity poses new security challenges for the mobile ecosystem, with broader attack surfaces, more devices, and greater traffic, the capabilities enabled by 5G and security features built into the standards for 5G architecture are poised to make 5G networks the most secure yet.

We do expect the United States to be the lead target for cyberattacks in the coming years – a clear call to action for all of us. We need networks that are trustworthy, resilient, and secure by design. We are at a fork in the road, and we have an opportunity for the U.S. to set a global example in 5G network security across policy, technology, and standards. Will the 5G world be innovative and dynamic? Secure and reliable? Will it enable fair competition and a robust marketplace necessary to protect national security? I believe that with intentionality and foresight, the United States will answer "yes" to each of these questions.

I want to share Ericsson's perspective on key priorities and key action items that will help guide us through this moment.

Ericsson serves customers in the U.S. and in more than 180 other countries, with over 100,000 employees worldwide – nearly 8,000 of whom are based in the U.S., at our headquarters in Plano, Texas. Although our global headquarters is in Sweden, a long-time U.S. partner and party to a formal cooperative defense agreement, the U.S. is effectively our "domestic" market, as it is our largest market, providing over one-third of Ericsson's global revenue, and it is also the market that drives our global R&D investments. Ericsson has a longstanding and growing commitment to the United States. Our presence in the U.S. dates back nearly 120 years and we have key development operations, as well as product, verification, and release activities, in North America. Ericsson also maintains strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies. In fact, all third party active "intelligent" electronics (e.g., digital semiconductors, silicon-based technology, application-specific integrated circuits (ASICs), field programmable gate arrays

(FPGAs), etc.) for the Ericsson Radio System (ERS) are predominantly sourced from U.S. companies, with a minor part from Japanese, Korean, and European companies.

We are actively expanding our investment in U.S. manufacturing and U.S. jobs. Last year we opened a $100 million 5G smart factory in Lewisville, Texas, where we are building Advanced Antenna System radios to enable rapid 5G deployments. We have four R&D locations in the US. We were the first vendor to launch 5G with all Tier-1 service providers in the U.S., and we are committed to helping to close the digital divide in rural America. Ericsson is also a global 5G leader. We led the way on 5G standards, with the highest share of 5G patent declarations – approximately 16.1 percent of essential 5G patent families – of any organization in the world.[1] More broadly, we are the largest holder of standard-essential patents for mobile communications, with 57,000 patents. Finally, we participate in more than 100 industry organizations, standards bodies, and other technology alliance groups.

Security is inextricably tied to the successful development and deployment of 5G networks, and we see three key priorities for enabling a successful and secure 5G rollout:

First, accelerating 5G deployment in the United States through increasing spectrum availability, especially mid-band spectrum; putting in place reasonable, streamlined small cell siting rules; and ensuring effective incentives to encourage 5G deployment in rural areas. This will give the U.S. the first mover advantage in 5G that it enjoyed in 4G – a meaningful step toward secure 5G. It will also ensure that the U.S. benefits from the extensive economic benefits that will come with 5G leadership, including an additional 4.5 million jobs and $1.5

[1] Christina Petersson, *When it comes to 5G patents, quality and essentiality matters* (Nov. 12, 2020), https://www.ericsson.com/en/blog/2020/11/5g-patents-quality-essentiality.

trillion in economic growth.[2] To that end, wireless and 5G infrastructure should play a prominent role in any government broadband programs, and should be funded in any broadband infrastructure funding legislation to ensure that rural areas are not left behind when it comes to 5G benefits, including mobility.

Second, strengthening and ensuring the long-term viability of a competitive, diverse global market of trusted and secure suppliers. Diversity in the network avoids "single point of failure" problems and also limits espionage and sabotage vulnerabilities. We all have a mutual interest in a diverse market – suppliers and service providers alike. U.S. Secretary of State Tony Blinken articulated the value of leveraging these strategic co-dependencies for the good of the U.S. and our partners and allies when addressing NATO earlier this year:

> We should bring together tech companies from countries like Sweden, Finland, South Korea, the United States, and use public and private investment to foster a secure and trustworthy alternative. We've spent decades developing relationships with countries that share our values in every part of the globe. This is why we invested so much in these partnerships – so we can come together in innovative ways to solve new challenges like these.[3]

To this end, the U.S. government should foster a diverse global market of trusted suppliers that are committed to delivering high performing, secure, and energy efficient network products to U.S. operators.

Third, supporting the important, ongoing work of standards processes and government-industry coordination. Ericsson is a leader in developing the standards for 5G security through the global 3rd Generation Partnership Project (3GPP), and we are engaged in

[2] Boston Consulting Group (BCG), *5G Promises Massive Job and GDP Growth in the US* (Feb. 2, 2021), *available at* https://www.ctia.org/news/report-5g-promises-massive-job-and-gdp-growth-in-the-u-s.
[3] Hon. Antony J. Blinken, Secretary of State, "Reaffirming and Reimagining America's Alliances," NATO Headquarters Agora (Mar. 24, 2021), https://www.state.gov/reaffirming-and-reimagining-americas-alliances/.

an effort through the Alliance for Telecommunications Industry Solutions (ATIS), supported by the Department of Defense (DoD), to develop standards for securing the 5G supply chain. We also serve on the O-RAN Alliance's Security Focus Group, which is in the early stages of developing Open RAN security specifications. These technical standards are crucial for security because they give all suppliers and carriers an open and transparent opportunity to identify and correct technical vulnerabilities, leading to effective network configuration and deployment. 5G is different from previous generations of wireless communications. Unlike the advances from 1G to 2G to 3G to 4G, 5G is a totally new and different technology and network architecture. 5G network functions will operate through a "virtualized" cloud-based network, allowing tailored security solutions for each different network function that will provide unprecedented capabilities for specialization in security for different isolated critical functions, for example, separating connected medical devices from less critical devices. These configurations in real-world deployments will be different in every case, but they should always be based on the rigorous, open and interoperable standards that Ericsson is helping to develop, and they should be bolstered by ongoing government-industry coordination efforts, such as the work of the FCC's CSRIC and the communications security initiatives that are underway through the leadership of the National Telecommunications and Information Administration (NTIA).

Ericsson commits significant resources to reach these goals. In short, we ensure that networks must, from the very start, be trustworthy, resilient, and secure by design.

First, in all of our manufacturing and software development facilities globally, Ericsson secures our own supply chain with tight quality controls, traceability and integrity checks, regular site audits, tests, and verifications. Additionally, in 2018 – prior to the disruptions

caused by the pandemic – we began executing a regionalization strategy for our supply chain, to place manufacturing and development as close to the customer market as possible in order to mitigate potential risks or regional disruptions and reduce dependence on one supply site or vendor. Particularly following the sophisticated compromise of SolarWinds' software supply chain, I want to emphasize Ericsson's approach to developing secure solutions. Well before the cyber attack on SolarWinds last year, all of our software was scanned, verified, cryptographically signed, and centrally distributed. We have strict software version control with check-in/check-out security, meaning that both the Ericsson employee who wrote the code and the individual who reviewed and accepted the changes are logged.

Ericsson supports the goals espoused in the President's Executive Order on Improving the Nation's Cybersecurity, which defines the term "Software Bill of Materials" or "SBOM" as a "formal record containing the details and supply chain relationships of various components used in building software."[4] Ericsson has vast experience in secure software development, through industry best practices such as the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF), which serves as one of our models for securely using proprietary, third-party, and open source software in development projects. As part of this process, Ericsson maintains internal SBOMs for its products and makes these available through a secure portal to customers on a contractual basis, protecting the confidentiality and authenticity of this important information. Furthermore, Ericsson evaluates its own software to identify vulnerabilities, utilizing static and dynamic code testing, privacy

[4] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 25, 2021) at Sec. 10 (j), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

impact assessments, scans at multiple deployment phases, code reviews, and penetration testing.

As policymakers and stakeholders advance the use of SBOM across diverse sectors and use cases, Ericsson has encouraged NTIA to develop SBOM requirements that build on our own work in software security assurance. In particular, we recommend that SBOM should be delivered in a controlled manner with limited distribution to only trusted third parties according to contractual agreements which should include confidentiality and integrity protection and mutual authentication during the transfer process. SBOMs should not be publicly disclosed, and SBOM requirements should be applied based upon the criticality rating of the software rather than in a "one size fits all" fashion. Ericsson has contributed this input and others to the June 2-3, 2021 NIST Workshop on Standards and Guidelines to Enhance Software Supply Chain Security as well as in written form to NTIA as part of its June 17, 2021 Request For Comments on Software Bill of Materials Elements and Considerations.

Second, we take a holistic approach to ensure that security is built into our systems from the start with layered due diligence and industry-aligned controls. We have developed an internal governance framework for security and privacy by design, providing guidance for security assurance across the product life cycle. Ericsson places top priority on protecting our customers' networks and their customers' data, as well as our intellectual property, all of which are governed under internal policies, and certified by ISO/IEC 27001, an international guideline on Information Security Management.

Third, in addition to our standards activities, we contribute to industry and government-industry initiatives to ensure supply chain and 5G security. These include our

service on the Executive Committee of the Communications Sector Coordinating Council (CSCC), best practice publications through the Council to Secure the Digital Economy (CSDE), leadership in NSTAC subcommittees and the aforementioned work on the ICT industry's response during COVID-19 as well as strategic planning for upholding the resilience of communications networks for the next decade, and our ongoing work in the FCC's CSRIC. Ericsson has been engaged across several working groups in the most recent iteration of CSRIC focused on 5G security and plans to participate fully in the upcoming CSRIC VIII. We are also participating in the groundbreaking work of the DHS ICT Supply Chain Risk Management Task Force, a formal, action-oriented collaboration between industry and government. I serve on the Threat Evaluation working group and I co-chaired a working group to develop methods for companies to provide formal assurances about their supply chain risk management, resulting in a Vendor Supply Chain Risk Management Template published in April. This will help make requirements such as the NIST security standards and other risk guidelines more useful in real-world acquisitions.

Fourth, with all of the above in mind, Ericsson heartily supports openness and the evolution to increasingly open network architectures. 3GPP has produced secure, open, and interoperable standards for each generation of cellular technology. 5G is the most secure generation of cellular networks that 3GPP has standardized to date, providing security end-to-end across the network through the RAN, core, transport and service-based architecture. Building on this work in 3GPP, industry is now working to develop technical specifications for Open RAN through the O-RAN Alliance and other technical collaborations.

While Open RAN is a nascent architecture, the benefits of Open RAN are evident in our own Cloud RAN portfolio, which focuses on hardware/software disaggregation, cloudification, open automation, and orchestration. Decoupling software and hardware allows RAN software to run on vendor-independent hardware, increasing vendor diversity. Increasing intelligence and automation allows operators to use tools to automate and simplify network operations on these decoupled, independent cloud platforms.

Ericsson is also a leader in the O-RAN Alliance. Ericsson co-chairs two working groups, made more contributions to O-RAN specifications in 2020 than any other company, and has the second-highest number of open source commitments and unique authors. Ericsson is currently supporting, or plans to support, eight of the ten RAN interfaces under discussion by the O-RAN Alliance. We urge the government to recognize the openness evident in the marketplace today, and to foreswear use of government mandates or preferences to drive the marketplace toward any particular technology. Instead of mandating or expressing a preference for a particular architecture, policymakers should continue to follow the longstanding guiding principle of technical neutrality and allow the industry to adopt the architecture of its choice based on the technology and business risks, without forcing the market to make investment decisions that could create significant deployment bottlenecks and other risks for U.S operators.

Ericsson believes that while Open RAN itself will not directly result in more secure networks, over time it can help provide benefits that advance security such as open interfaces, cloudification, intelligence, and automation to enable increased vendor diversity, deployment flexibility, higher performance, and greater resiliency in the 5G RAN. In this nascent stage of

development, however, this new architecture may, in fact, create new security risks. Accordingly, Ericsson is providing leadership in the O-RAN Alliance's Security Focus Group, which has adopted official work items to address new security risks unique to O-RAN, and we have recently been appointed as its liaison to the GSMA Fraud and Security Group.

Regarding policy to facilitate Open RAN's development and deployment, Ericsson itself sees no barrier to deploying Open RAN solutions. Ericsson's Cloud RAN is a major step on the journey to a secure Open RAN solution that meets the needs of U.S. critical infrastructure. It allows operators to run Ericsson RAN software using non-Ericsson open hardware and the third-party cloud stack (e.g., platforms provided by IBM/Red Hat, Linux, HPE, Intel, and many others). Ericsson has every reason to ensure that the regulatory environment is not unfavorable to our own Open RAN products. We can find nothing that would impede Ericsson or any other vendor from competing in the marketplace for Open RAN products and services.

Finally, what can the Committee do to support all this? First: Pass, implement, and oversee legislation to promote wireless security. We commend Committee Members for developing and engaging with industry on the proposed legislation that is the subject of this hearing, and we look forward to working with you on these bills as you consider them.

Second: Support actions to accelerate 5G deployment. Accelerated 5G deployment will advance the security of the 5G supply chain. Again, wireless and 5G infrastructure should qualify for funding in any broadband infrastructure funding legislation. The U.S. has the most innovative and competitive high-tech marketplace in the world, and a major key to that success is the fact that the market determines which technologies win, and which lose. Governments tipping the scales in the technology arena generally do not generate desired outcomes, and it

would be a mistake to push innovators onto any particular technological path—especially in an area in which technical specifications are still being developed. Ericsson thus asks that the Committee support technological neutrality, rather than requirements or preferences designed to push the market toward any particular type of network deployments.

Third: Continue to enable a secure and robust marketplace of trusted suppliers. Because global and domestic security are intertwined, it is imperative to ensure the long-term viability of a competitive, diverse global market of trusted and secure suppliers. The Committee should recognize and promote the value of leveraging strategic co-dependencies among the U.S. and its partners and allies, and develop policies that foster a diverse, trusted, global market of suppliers that deliver high performing, secure, and energy efficient network products to U.S. operators.

Fourth: Keep holding hearings on the subject of 5G security. Hearings like this highlight what industry and government agencies are doing to ensure a secure 5G world and maintain pressure on us to stay true to our security commitments.

* * *

On behalf of Ericsson, I thank the Committee for its leadership in this area. We look forward to continuing to work with you, and I look forward to your questions.

Mr. DOYLE. Thank you, Mr. Boswell.
Mr. Brenner, you have 5 minutes.

STATEMENT OF DEAN R. BRENNER

Mr. BRENNER. Thank you.

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 leading supplier of chips, an entire modem-RF system, for smartphones, tablets, always connected laptops, cars, WiFi access points, and more, and the world's leading inventor and licensor of new wireless technologies.

We are working on 5G at a feverish pace. It is rolling out far more rapidly and broadly than any prior wireless technology. There are over 165 operators providing 5G in over 60 countries and nearly 1,000 5G devices that have been announced in development or for sale using our modem-RF system. Over 80 devices for 5G fixed wireless access use our solution too.

Let me thank this subcommittee for enacting the Emergency Broadband Benefit, which is providing discounted connectivity and equipment to over 3 million low-income households, and the Emergency Connectivity Fund, which will provide devices and connectivity to millions of K–12 students.

COVID has made it clear that everyone must have a device and connectivity. It is essential that we solve the digital divide—a 50-State urban-suburban-rural problem, especially for students and teachers, once and for all.

Thank you also for years of collaboration over the key input we need for all of our technologies: spectrum. We don't just sit back and wait for new spectrum. Rather, our technical and standards work takes place in parallel with our spectrum initiatives so that, when new spectrum is allocated, we can put it into chips quickly to get it right into the hands of consumers.

When the FCC allocated the 6 gigahertz band for WiFi and other technologies last year, we had chips using that band ready to go. Likewise, the FCC optioned the C-band spectrum, and when it starts coming into use late this year, we will have chips for the band. Now, we are working on new versions of 5G with many enhancements, but also on spectrum initiatives, to enable improved use of lower 37 gigahertz, 5.9 gigahertz, 60 gigahertz, and other bands too.

American leadership and wireless depends on continuing technological innovation but also freeing up a steady stream of more low-, mid-, and high-band spectrum. Doing so requires continuing the close collaboration among this subcommittee, the FCC, NTIA, other policymakers, the wireless industry, and others, and that is what we plan to do.

Let me provide Qualcomm's perspective on three key topics covered by the nine bills in front of you today. The first is 5G security, which has always been a top priority for Qualcomm. Qualcomm works on 5G security internally, with other companies, and in 3GPP, which sets 5G standards.

Also, for many years, Qualcomm has been an active participant and leader in CSRIC, the FCC's Communications Security, Reli-

ability, and Interoperability Council. In 2019, the chairman and ranking members of this subcommittee and the full committee asked then-FCC Chairman Pai that CSRIC examine 5G security. Subsequently, one of Qualcomm's engineers, Dr. Farrokh Khatibi, was appointed to lead the CSRIC working group on that issue. We look forward to continuing our leadership efforts in the next CSRIC.

The second topic is open RAN. Qualcomm is a leader in developing open RAN, which allows a more diverse group of suppliers to provide innovative, reliable, secure, and trusted cellular infrastructure at lower cost. We are actively participating in industry efforts to advance an open RAN ecosystem through research and development, standardization, testing, and security. We are working closely with operators and infrastructure manufacturers globally to help drive open RAN deployments.

This week, we announced the world's first 3GPP Release 16 5G open RAN platform for small cells, which supports open and virtualized RAN, open RAN for sub-6 gigahertz and millimeter wave bands to facilitate scaleable and cost-effective 5G networks across all bands. Our new platform will help drive open RAN with flexible and open architectures and power efficiency. We also announced a 5G Distributed Unit Accelerator Card, which is going to simplify the deployment of 5G virtual networks.

The rapid deployment of open RAN goes hand-in-hand with the increasing densification of wireless networks. Densification is accelerating sharply in 5G, especially in millimeter wave bands, which enable multigigabit, ultralow latency, ultrareliable communication to fill in 5G's true potential. That is why 43 companies around the world joined us this week to announce their support for 5G millimeter wave.

Finally, the last topic is 6G. Even while working on enhancing 5G, we have begun to work on 6G in a very early research-an-development phase and to work with NTIA and potential spectrum bands for testing. One focus will be on spectrum in the 7-to-24-gigahertz range for wide coverage. Identifying and freeing up such bands will be a multiyear effort. We are also working in industry groups that are beginning to discuss 6G. I am quite confident that Qualcomm will lead the way on 6G.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Brenner follows:]

Before the

United States House of Representatives

Subcommittee on Communications & Technology

Hearing on

"A Safe Wireless Future: Securing Our Networks and Supply Chains"

Testimony of

Dean R. Brenner

Senior Vice President, Spectrum Strategy & Tech Policy

Qualcomm Incorporated

June 30, 2021

Chairman Doyle, Ranking Member Latta, and Members of the Subcommittee, my name is Dean Brenner, and I'm here 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, tablets, always connected laptops, cars, Wi-Fi access points, and more, and the world's leading inventor and licensor of new wireless technologies. We are working on 5G at a feverish pace. 5G is rolling out far more rapidly and broadly than any prior wireless technology. There are more than 165 operators providing 5G in over 60 countries, and nearly 1,000 5G devices have been announced, are in development, or for sale using Qualcomm's modem-RF system. Over 80 devices for 5G fixed wireless access use our solution too.

Let me thank this Subcommittee for enacting the Emergency Broadband Benefit, which is providing discounted connectivity and equipment to over 3 million low-income households, and the Emergency Connectivity Fund, which will provide devices and connectivity to millions of K-12 students. COVID has made it clear that everyone must have a device and connectivity. It is essential that we solve the digital divide—a 50-state, urban-suburban-rural problem, especially for students and teachers—once and for all.

Thank you also for years of collaboration over the key input we need for all of our technologies: spectrum. We never just sit back and wait for new spectrum. Rather, our technical and standards work takes place in parallel with our spectrum initiatives so that when new spectrum is allocated, we can put it into chips quickly to get it into the hands of consumers. When the FCC allocated the 6 GHz band as an unlicensed band for Wi-Fi and other technologies last year, we had chips using that band ready to go. Likewise, the FCC auctioned the C band spectrum in February 2021 and when it starts coming into use late this year, we'll have chips supporting the band. Now, we're working on new versions of 5G with many enhancements, but also on spectrum initiatives to enable improved use of Lower 37 GHz, 5.9 GHz, 60 GHz, and other bands too.

American leadership in wireless depends on continuing technological innovation, but also freeing up a steady stream of more low, mid, and high band spectrum. Doing so requires continuing the close collaboration among this Subcommittee, the FCC, NTIA, other policymakers, the wireless industry, and many other stakeholders, and that is what we plan to do.

Let me provide Qualcomm's perspective on three key topics covered by the nine bills before you today. The first topic is 5G security, which has always been a top priority for Qualcomm. Qualcomm works on 5G security internally, with many other companies, and in the 3GPP global standards group which sets 5G standards. In addition, for many years, Qualcomm has been an active participant and leader in CSRIC, the FCC's Communications Security, Reliability & Interoperability Council.

In 2019, the Chairmen and Ranking Members of this Subcommittee and the full Committee asked then-FCC Chairman Pai that CSRIC examine 5G security. Subsequently, one of Qualcomm's engineers, Dr. Farrokh Khatibi, was appointed to lead the CSRIC Working Group on that issue. We look forward to continuing our leadership efforts in the next CSRIC.

The second topic is Open RAN. Qualcomm is a leader in developing Open RAN, which allows a more diverse group of suppliers to provide innovative, reliable, secure, and trusted cellular infrastructure at lower cost. We are actively participating in industry efforts to advance an Open RAN ecosystem through research and development, standardization, testing, and security. We are working closely with operators and infrastructure manufacturers worldwide to help drive Open RAN deployments.

This week, we announced the world's first 3GPP Release 16 5G Open RAN platform for small cells, which supports open and virtualized RAN for sub-6 GHz and millimeter wave bands to facilitate scalable and cost-effective 5G networks spanning all spectrum. Our new platform will help drive Open RAN with flexible and open architectures and power efficiency. We also announced a 5G Distributed Unit Accelerator Card, which will simplify deployments of 5G virtualized networks.

The rapid development of Open RAN goes hand-in-hand with the increasing densification of wireless networks. Densification is sharply accelerating in 5G, especially in millimeter wave bands, which enable multi-gigabit, ultra-low latency, ultra-reliable communication, fulfilling 5G's true potential. That's why 43 companies around the world joined Qualcomm this week to announce their support for 5G millimeter wave.

The last topic is 6G. Even while we continue to work on enhancing 5G, we have begun to work on 6G in an early research and development phase, and to work with NTIA on potential

spectrum bands for testing. One focus will be spectrum in the 7 to 24 GHz range for wide coverage deployments. Identifying and freeing up such bands will be a multi-year effort. We are also participating in industry groups beginning to discuss 6G. I am quite confident that Qualcomm will lead the way on 6G.

Thank you, and I look forward to your questions.

Mr. DOYLE. Thank you, Mr. Brenner.
Mr. Johnson, you are recognized for 5 minutes.

STATEMENT OF CLETE D. JOHNSON

Mr. JOHNSON. Thank you so much, Chairman Doyle and Ranking Member Latta, Ranking Member McMorris Rodgers, Members. I thank you for the opportunity to join you here in person. It is a delight.

Having been in the policy trenches on communications security issues through many administrations and Congresses, I am especially grateful for your bipartisan approach. In my work in the Senate, at the FCC, at Commerce, within the NSC, and now in private practice, I have been involved in nearly every cybersecurity policy development since the Bush administration.

Through Presidents Bush, Obama, Trump, and now Biden, the clear trajectory of cybersecurity policy is, first, industry leadership and, second, industry partnership with a well-coordinated Federal interagency. Successive Congresses and administrations have put the cornerstones of this approach in place, beginning with NIST foundational cybersecurity framework and cyber threat information sharing legislation. And then since then, many more new laws and activities and initiatives at Commerce, CISA, and the FCC. These precedent-setting initiatives all promise to advance industry leadership and government industry partnership for secure, reliable communications.

Following recent attacks on SolarWinds and Colonial Pipeline, we are now entering a new phase. We must fully operationalize the foundational policies and partnerships developed over the past 15 years.

I think the central question here is the crucial relationship between the ICT industry and the Federal Government. Will the future be prescriptive regulation or collaborative partnership?

Today, I urge the subcommittee to consider exactly why the partnership will produce superior outcomes against the common threats we face. Government and industry must be on the same team to defend against the sophisticated adversaries that target all of us.

As Mr. Boswell noted, the pandemic has shown that the ICT industry collectively constitutes our single greatest asset for secure, reliable connectivity. The ICT industry in the United States has the most sophisticated and well-resourced security operations in the world. During the unprecedented demands of the pandemic, when every single day it was Mother's Day or New Year's Eve with regard to communications traffic, the ICT industry's core interest in maintaining connectivity was an indispensable imperative. It always is. This industry imperative not only fully aligns with the U.S. Government's interest in network security, it is actually the foundation of defending that Government interest.

That is why in those harrowing months when our world changed completely, the FCC, CISA, and many others turned to network operators to keep our society functioning. This collaborative effort was not a regulatory mandate. Nobody told industry what they had to do. Instead, Government officials were asking companies how the Government could help them keep our society connected. It was

a partnership that was as urgent as the lifesaving and life-sustaining activities that depended on it, and it worked.

This is the model for the future, because U.S. network operators and their trusted suppliers are the U.S. Government's most important partners in securing our Nation's networks.

Unlike other critical infrastructure sectors, the ICT industry has been working with the Government on secure, reliable connectivity for decades, really going back to the height of the Cold War when President Reagan—under the threat of nuclear weapons disrupting our communications capabilities, President Reagan established the predecessors of today's government/industry partnerships.

Put simply, the ICT industry knows how to work with government to ensure the security and reliability of the Nation's networks. Today's new challenges and opportunities call for deeper and more efficient partnerships to help network operators and their trusted suppliers defend the country.

The ICT industry needs the Government to advance these partnerships, especially with Commerce, the FCC, and CISA. They need coordinated processes that leverage industry strengths, minimize duplication and turf battles, and maximize coordination and impact.

When I was at the FCC in 2015, the communications sector provided an innovative path to this goal with groundbreaking CSRIC recommendations for FCC–DHS partnership with network operators. It was a new paradigm. It was industry-led cooperation with government, perhaps an idea before its time as it got bogged down in FCC–DHS turf wars. But it is not too late to get this right.

Given the maturation of interagency processes, the increasingly clear authorities of Commerce and CISA, and the FCC's recognition that its most meaningful role is in supporting the interagency, the time is now ripe for the U.S. Government to work with the ICT industry to take big steps in securing our networks. The bills you are considering today can help us get there.

I look forward to answering your questions. And thank you again.

[The prepared statement of Mr. Johnson follows:]

Testimony of Clete D. Johnson

Senior Fellow,
Center for Strategic and International Studies

Partner,
Wilkinson Barker Knauer, LLP

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

Hearing on

A Safe Wireless Future: Securing our Networks and Supply Chains

June 30, 2021

Chairman Doyle, Ranking Member Latta, Chairman Pallone, and Ranking Member McMorris Rodgers, Members of the Committee, thank you for the opportunity to join you – in person! – today to share my views on the best path toward a future of secure and reliable wireless communications.

Having been in the policy trenches on these issues through many different Administrations and Congresses, I have special gratitude for the Committee's bipartisan approach to cybersecurity, supply chain security, and the bills that are the subject of this hearing. Thank you.

In my work in the Senate, at the Federal Communications Commission (FCC), in the Commerce Department, within the interagency processes of the National Security Council, and now in private practice and in the think tank arena, I have been personally involved in just about every major cybersecurity policy development since the end of the Bush Administration. Since cybersecurity became a prominent federal policy issue in the late 2000s – through the Administrations of Presidents Bush, Obama, Trump, and now Biden – the clear trajectory of cybersecurity policy is steady progress toward industry leadership and partnership with a well-coordinated federal interagency.

Successive Congresses and Administrations have put the foundational cornerstones of this policy approach in place:

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Cybersecurity Enhancement Act that codified NIST's private sector engagement model;

- The Cybersecurity Information Sharing Act that provided new clarity and safeguards for operational sharing of cyber threat indicators;

- The Secure and Trusted Communications Networks Act and related appropriations, through which the FCC is reimbursing the replacement of untrusted equipment in subsidized networks;

- The Secure 5G and Beyond Act, which prompted the development of the National Strategy to Secure 5G;

- The provisions of last year's National Defense Authorization Act, which created the Public Wireless Innovation Fund, to be administered by the National Telecommunications and Information Administration (NTIA) to promote breakthrough advances in promising areas such as Open Radio Access Network (RAN) architecture;

- The Commerce Department's work with industry to secure the hardware and software supply chain; and

- The work of the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) on 5G security, and the FCC's related supply chain security proposals.

All of these are precedent-setting initiatives. They all have the promise of further advancing industry leadership and government-industry partnership.

Building on this foundation, and particularly following recent attacks on SolarWinds and Colonial Pipeline, we are now transitioning to an altogether new phase of cybersecurity and supply chain security policy. We are no longer establishing the foundations of this policy; now, we must fully implement, operationalize, and build on the policies and partnerships we have developed over the past fifteen years.

Perhaps the central "next step" question pertains to the crucial relationship between the Information and Communications Technology (ICT) industry and the federal government on cybersecurity and communications reliability. Will the future be prescriptive regulation or collaborative partnership?

I urge the Committee to consider that collaborative partnership across the ICT industry will produce superior outcomes against the common threats we face. Government and industry must be on the same team to defend against the sophisticated adversaries that target all of us, and I know from my time as the FCC's Chief Counsel for Cybersecurity that regulatory agencies can be extremely influential in enabling – or alternatively, in blocking – this necessary teamwork.

One of the lessons learned from the COVID-19 pandemic is that the network operators, trusted suppliers, and other stakeholders of the ICT industry collectively constitute our greatest national asset towards the goal of secure, reliable connectivity.

The ICT industry that serves the United States has the most sophisticated and well-resourced security operations in the world. As demonstrated during the unprecedented connectivity demands of the pandemic – when every single day was Mother's Day and New Year's Eve with regard to telecommunications traffic – the ICT industry's core interest in maintaining secure, reliable connectivity is an indispensable imperative.

This industry imperative not only fully aligns in every way with the U.S. government's interest in network security – it is in fact the foundation of defending that government interest.

That is why throughout the pandemic, particularly in those harrowing early months when our world changed completely, the FCC, NTIA, the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and other government agencies turned to network operators and the broader ICT industry to keep our society connected and operating.

This collaborative effort was not a regulatory mandate or government otherwise telling the ICT stakeholders what they had to do. Instead, government stakeholders were asking ICT stakeholders how the government could help them keep our society connected during the crisis. It was a partnership that was as urgent as the life-saving and life-sustaining activities that depended on it. And it worked.

This is the model to follow in the future, because U.S. network operators and their trusted suppliers are the U.S. government's most important partners in securing our nation's networks.

Unlike other critical infrastructure sectors, the ICT industry has been working in close partnership with the government to maintain secure, reliable connectivity for decades, going back to the height of the Cold War when – under the threat of nuclear weapons disrupting our communications capabilities – President Reagan established the predecessors of today's public-private National Coordinating Center for Communications, a joint government-industry operation hosted at DHS CISA, and the Communications and IT Sector Coordinating Councils.

In short, the ICT industry knows how to work with the government to ensure the security and reliability of the nation's networks. New challenges and opportunities, from IoT to 5G security to Open RAN to incident detection and response, call for deeper and more efficient partnerships to help network operators and their trusted suppliers help the country.

The ICT industry needs the government to advance existing partnerships – particularly with the Commerce Department (both NTIA and NIST), the FCC, and CISA. They need coordinated interagency processes that leverage industry's strengths. They need careful U.S. government attention to minimize duplication and turf battles, and to maximize coordination and impact.

When I was at the FCC in 2015, the communications sector provided a path to this goal via its groundbreaking CSRIC recommendation that the FCC partner with DHS to engage in partnership with network operators. It was a "new paradigm" of industry-led cooperation with government – perhaps an idea before its time, as the idea bogged down in FCC-DHS turf wars. However, particularly given our nation's experience maintaining secure, reliable connectivity throughout the pandemic, I am confident we have grown past those turf battles at this point.

Given the maturation of interagency processes that have developed since that time, particularly the increasingly clear authorities of the Department of Commerce and CISA, as well as the FCC's recognition that its most meaningful role is in supporting interagency processes rather than taking unilateral actions, the time is now ripe for the U.S. government to work with the ICT industry to take the next big steps in securing our nation's networks.

The bills you are now considering can help make that happen, so long as we continue close partnership between industry and government.

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

Mr. DOYLE. Thank you, Mr. Johnson.

We have now concluded opening statements. We are going move to Member questions. Each Member will have 5 minutes to ask questions of our witnesses.

I want to thank both Ranking Member Latta and McMorris Rodgers for their brevity in their opening statements. Since I recognized it to the panelists, it is only fair that you get some—doesn't get you any extra time on your questions, but I just wanted to thank you.

So I will start by taking 5 minutes for my questions.

Mr. Brenner, you write that, even as Qualcomm continues to work on enhancing 5G, you have also begun to work on 6G in an early research-and-development phase, engage with NTIA regarding 6G, and are participating in industry groups to discuss the emerging standard. Tell me, how would a 6G task force at the FCC be useful to industry and to the country?

Mr. BRENNER. Thanks very much, Chairman Doyle, for your question. And I want to be very clear: We are in a very early phase of 5G. We have two versions of 5G that have been completed in the Sanders process. We are on our third-generation modem. We are working on the third version, fourth version. So there is a long runway for 5G, but we work with tremendous urgency at Qualcomm. We are not holding our breath waiting for a task force. We are chugging along. So we have begun in an early phase to look at 6G, to begin working on it, and to get ready to start doing some early testing of it.

So what I liked about your task force is—are two things: A, that it should be centered at the FCC. The FCC, at the end of the day, is going to have to allocate spectrum for 6G, and as I explained in my testimony, there isn't going to be 6G without spectrum, and the spectrum and technology interactions, they have got to take place at a very early stage. So that was point one.

And then point two, siting. So you—in the bill, I noticed that one of the things that this task force would work on is siting. The 5G millimeter wave, which I referred to in my testimony, it delivers 5G 16 times faster than 5G in a lower band. So, you know, people all over the United States, in all of your districts, they should get 5G millimeter wave, but to do that, we do need more sites. And it is never too early to, you know, to have collaboration over where to put these sites so that States and localities don't just sort of wake up and say, "Oh, my God, what this is 6G stuff?"

Mr. DOYLE. Sure. Just to put it in perspective, as the world began preparing for 5G, what components of leadership were necessary? And how long did it take between the start of 5G development and 5G deployment?

Mr. BRENNER. Yes. That is also a great question, and I can certainly remember when 5G was on a whiteboard, and that is how all of our technologies start. You know, there is a—you know, and the other part of this is every government in the world wants their country to be the leader in 5G. You know, we are Qualcomm. As I said, we are based in San Diego, but we are a global company. We have offices everywhere. I have colleagues all over the world.

So, you know, it is a 5-, 6-, 7-, 8-year process to design, test, and get global consensus around a wireless technology, and then, in

parallel on our product side, get the chips ready to go so that, when the spectrum is allocated and the standard is finished, the chips can roll out into consumers' hands.

Mr. DOYLE. Well, thank you.

Mr. Boswell, as you may know, last week, I introduced the FUTURE Networks Act, along with Congressman Johnson and Congresswoman McBath. Do you support that bill, and would you share your views on the importance of focusing on 6G while we role out 5G?

Mr. JOHNSON. Thank you. As my colleague here——

Mr. DOYLE. Is your microphone on?

Mr. JOHNSON. I am sorry. Wow, I will get this microphone—it has been 15 months. Wow, this is like our new version of Skype and Teams' mute button, I guess, now.

But, thankfully, if we had not already started on this race to 6G, frankly, we would already be behind, but industry has been investing heavily in this for quite a bit. Each cycle in a cellular generation is about 8 to 10 years. To give you a sense of how important 6G is to us at Ericsson, we are already hard at work on related research and testing to ensure a leadership position for the U.S.

In addition to our own R&D, it is important to recognize different collaborative efforts, either with government or with others in the private sector. We are a founding member of the National Science Foundation RINGS program—that is the Resilient and Intelligent Next-Generation Systems program—which seeks to accelerate research in areas with potentially significant impact on next-generation networking and computing. So that will be artificial intelligence, quantum computing, quantum cryptography, kilohertz spectrum, lots of different things that we will need to take advantage of 6G, not just make it go faster.

There is also work we are doing with NSF's platform for an advanced wireless research program and the ATIS' Next G Alliance. All of these are very important to have private-public collaborative partnerships to help advance 6G, and America is already on that path.

Mr. DOYLE. And, Mr. Boswell, I have to stop you there as my time has expired and I want to set a good example for my colleagues.

Mr. BOSWELL. Thank you, Chairman.

Mr. DOYLE. The Chair now yields to the ranking member, Mr. Latta.

Mr. LATTA. Thank you very much, Mr. Chairman.

And, again, thanks to our witnesses for being here.

Mr. Brenner, if I could start my questions with you. Qualcomm has participated in 3GPP virtually since its inception in the late 1990s. A decade later, contributions made in 3GPP by the U.S. and like-minded countries helped America lead in 4G deployment. Today, Qualcomm and other trusted companies are working in 3GPP to continue work on the 5G and now 6G standards.

Would you speak about the role the private sector and the role of government in making sure we are ready to lead in the 6G here in the United States? And it is kind of interesting that there is across the witnesses and I think some of the questions you are going to hear today is about that private-public partnership and

working together and not having the heavy hand of government, I think, out there so you can all get out there and do what you need to do.

Mr. BRENNER. Thanks you very much, Ranking Member Latta. And, you know, Qualcomm wouldn't exist if there were a heavy hand in government. We started our first technology in 2G, and there were three 2G technologies and, fortunately, the FCC decided that they shouldn't pick the technology; let the market decide. And then our technology was able to lead the way into 3G, 4G, and 5G. So we are very attuned to this question of what the proper roles are.

The FCC—an FCC task force is not going to invent 6G. They are not going to design 6G technology. That is what we are going to do, not by ourselves, interacting with all of our partners all over the world, Ericsson, a zillion other companies. But what can government do? Well, our technology, as I explained, it can't get into the hands of a customer without spectrum. Our technology, we can't make a chip unless the Government support the semiconductor industry.

So, you know, again, for sites, you know, you can have the greatest phone in the world, but if there is not a bay station that you can connect to, your phone is going to be, you know, unusable. Or WiFi access point.

So government has a clear role. It is in the areas of spectrum, siting, and then closely interacting with the private sector. We don't want 5G to be a surprise to the FCC. It hasn't been. The FCC participates in 3GPP. Other parts of the U.S. Government—NTIA, the Department of Transportation, the Defense Department—they all need to know what these technologies are as they are evolving and being standardized.

So that is really how I see the differing roles between the private sector and the public sector.

Mr. LATTA. Well, thank you.

Mr. Johnson, you have worked on cybersecurity and supply chain issues in the communications industry across an array of roles in the Federal Government. There are a few bipartisan bills before us today led by Republican Members that seek to improve policy coordination and communication with the private sector. Do these bills strike the appropriate balance for the public-private sector responsibilities?

Mr. JOHNSON. Thank you, Congressman. As I said, I think this is the central big-picture question of this issue, and I do think that the bills before us, not to take three—each one—but they all have that partnership and the interagency coordination in mind.

We have grown up quite a bit since, you know, cybersecurity policies sort of became an issue in, say, 2006, 2007. It was—at that point, DHS was brand new. The Commerce Department was not engaged in the same things that they are engaged in now, and the FCC's authorities were really—let's just put it bluntly—the FCC's relationship with the internet was a contentious issue.

Now, we have a much more clear understanding of who can do what and how and how—most importantly, how they work together to maximize the industry's expertise, as Mr. Brenner said.

Mr. LATTA. Let me follow up. Do you have any suggestions—in my last 51 seconds here, the chairman might have me drop through the floor—that we may consider strengthening public-private partnership in advancing the U.S. communications security—and security?

Mr. JOHNSON. I think this committee has—and kudos to you for putting these bills forward. I think this committee's emphasis on the Commerce Department is very important, and its emphasis on the FCC's activities and pulling in industry, for instance, through the CSRIC, is critical.

The Commerce Department is a really interesting agency of government, and you think about—you think about an NSC meeting where you have 20 or 30 different representatives of all agencies of government, mostly security agencies, and then there is the guy or gal from the Commerce Department, who is the only person there that works for the Department, whose core mission is advancing U.S. business and innovation. That is a crucial part of securing our networks, and that voice is a very important part of the security environment.

Mr. LATTA. Well, thank you very much.

Mr. Chairman, my time has expired, and I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. McNerney for 5 minutes.

Mr. MCNERNEY. Well, again, and I thank the chairman.

I thank the witnesses. Your expertise is appreciated, and your willingness to work with us is also deeply appreciated.

I want to talk about H.R. 4028 that I introduced along with Representatives Long and Spanberger. It is called the Information and Communication Technology Strategy Act, which you are considering today. It would require, among other things, the Commerce Secretary to submit a whole-of-government strategy to ensure competitiveness of trusted vendors in the United States.

I think this bill is necessary to ensure that we are thinking about the future supply chain and what to do about the robust marketplace for communication equipment.

So, Mr. Johnson, given your experience with the Federal Communications Commission, at the Commerce Department, within the interagency process of the National Security Council, you have a very unique perspective into the security capabilities of the communication networks. Why is the Commerce Department the best agency to take lead on this work?

Mr. JOHNSON. Thank you, Congressman. I appreciate that, and I would like to acknowledge that one of the people that was core in building these foundations is your son, who was previously at the Defense Department, now an innovator in Silicon Valley. So he is part of this thriving ICT industry.

Mr. MCNERNEY. Well, thank you.

Mr. JOHNSON. To follow up what I was saying before, the Commerce Department is unique in the Government. You might say the Small Business Administration does similar work. But as a Cabinet-level agency, it is the only agency whose core purpose and whose employees wake up in the morning trying to promote business and innovation, both in the United States and through U.S. companies worldwide.

So it has—and I think Secretary Raimondo has already taken this charge. It has a core role in promoting the digital economy, which is core to the—obviously, to the cybersecurity, promoting digital services through the International Trade Administration, of course, spectrum issues and other telecommunications and internet policy at NTIA, and NIST is the world's experts in standards in technology. The Bureau of Industry and Security is playing an increasing role in preventing untrusted suppliers from being part of our markets.

So I think the Commerce Department is crucial as part of this team to go along with the FCC and DHS CISA.

Mr. MCNERNEY. What are the special challenges then with the meeting whole-of-government strategy?

Mr. JOHNSON. I think the challenges—not to be too glib about it, the challenge is that humanity is stovepiped and territorial. And so you have to—in order to create true joint interagency teams, you have to get past that sort of human weakness of people wanting to be in charge of things. Like I said——

Mr. MCNERNEY. Sort of the jurisdictional issues that we have here.

Mr. JOHNSON. So that is a big challenge, but I will tell—what I do think has happened is, in real world—and this why I go back to the pandemic and also response to SolarWinds, response to Colonial Pipeline—real-world necessities drive improvements, and we have seen that through WannaCry 4 years ago, through the Iranian DDoS attacks on our banks 8 years ago. Real-world activities force officials and agencies to get things right, and I think we have seen a lot of maturation in those recent years.

Mr. MCNERNEY. Well, I want to ask about CSRIC, but I only have 1 minute left. So I want to move on to another question.

Mr. Srihari, you draw a distinction in your testimony between open RAN and open network architecture. Could you please elaborate on that a little bit? And I will be sending questions for the record.

Mr. SRIHARI. Sure. Well, open RAN is a subset of open network architectures. Open network architectures refer to the concept of taking a traditional network element, like a bay station or a router, breaking it apart into its constituent pieces, and connecting those pieces through common interfaces. RAN is just the radio access network, the part where your mobile device connects to the tower. But there is also the transport, the backhaul to get the signal from the tower back to the core central office, as well as the core. All of those things can be open and disaggregated.

And so when I speak about open network architectures, what I really mean is disaggregating and enabling competition by breaking apart all of the pieces of the network from end to end, not just the radio access network piece on the edge.

Mr. MCNERNEY. So I appreciate the chairman's discipline on time except when it is my turn to talk.

And I yield back.

Mr. DOYLE. I thank the gentleman.

The Chair now recognizes Mrs. Rodgers for 5 minutes.

Mrs. RODGERS. Thank you, Mr. Chairman.

Mr. Brenner, Qualcomm is a trusted company. Plays a large role in international standard-setting bodies like 3GPP. There have been efforts by this committee and across Congress to enhance participation by U.S. companies in international standard-setting processes in order to push back against adversarial countries trying to impose their policies on the rest of the world.

Mr. Brenner, what is the role played by Huawei in these bodies? And how does their participation impact conversations?

Mr. BRENNER. So thank you for that question. It is actually a very complex question because of the fact that, you know, as a global leader in the wireless industry, we have interaction with every company in the wireless industry, including the company that you mentioned. We have those interactions for a couple reasons. One is at the end of the process, you know, we want to have Qualcomm chips get into smartphones and all those other devices I mentioned all over the world, including in China and other places where adversarial countries are based. We have a large group of employees who work in China too. And so we do need to make sure that our phone with a Qualcomm chip is going to work with infrastructure, no matter whether it is infrastructure made by whoever.

On the other hand, in the standards process, you know, it is usually a meritocracy. The best technical ideas through a consensus-driven process are usually the ones that prevail. However, the geopolitics does, you know, enter into those things. There are, you know, times when, you know, when Huawei, when we don't have—you know, it is not like we have conflict with them over every single issue. And, in fact, it is a vast minority of issues in 5G, for example, where Huawei may have a different view than we do.

And, you know, what we have to do is, you know, we don't have the option of just withdrawing and just taking our—you know, taking our toys and going home, so we have to interact with companies all over the world and convince them that the ideas that we have are the best ones to make the technology the best.

Mrs. RODGERS. Right. So important.

Mr. Boswell, last October, Sweden enacted a 5G equipment sales ban against Chinese companies Huawei and ZTE, following suit taken by actions in the United States to secure our networks from foreign bad actors. Just last week, the Stockholm administrative court upheld this action. Over the last several months, it has been reported that your CEO lobbied against this ban in Sweden, which runs counter to the actions taken by the United States to push allied countries to remove this equipment.

Given the topic of today's hearing, I am concerned that Ericsson, one of the top trusted vendors in the United States, appears to be taking a different position on Huawei than the U.S. Government. How does Ericsson engage with Huawei when discussing cyber security or developing standards for equipment? And do you agree that Huawei equipment poses a national security threat in our networks?

Mr. BOSWELL. Well, I can't speak for—and I would like to point out I figured out the mute button thing, by the way. Yes, but I can't speak for any government, foreign or domestic. I am not a diplomat. I am an engineer. My job is to secure networks, secure our solutions, and to secure U.S. infrastructure, frankly. We don't

source anything from Huawei or ZTE, so I can't speak to specifics on that.

As far as what Mr. Brenner mentioned about standards bodies, of course, we work with dozens or even hundreds of companies across different standards organizations, but I am afraid that is all I can comment on about that.

Mrs. RODGERS. This committee has a history of working together, especially when it has come to enhancing our network security. We worked together to pass the Secure and Trusted Communications Network Act to get Huawei out of our networks. Just last year, we worked to pass the U.S. Telecommunications Act to promote the development of open RAN compatible technology. While open RAN shows promise to increase vendor diversity, we also recognize it is a new concept.

So, Mr. Boswell, I just would like you to comment on H.R. 4032. So that is the legislation before the committee, the Open RAN Outreach Act, which would establish a government office to provide technical assistance to smaller companies interested in deploying open-RAN-compatible technologies. And what role do you think the Government should play in the development of open RAN?

Mr. BOSWELL. Well, I only have about 8 seconds——

Mrs. RODGERS. Yes.

Mr. BOSWELL [continuing]. I see here.

Mrs. RODGERS. Yes.

Mr. BOSWELL. So perhaps I will submit an answer for the record for that, or I could continue.

Mrs. RODGERS. OK.

Mr. DOYLE. That will be fine. You can submit it for the record.

Mr. BOSWELL. Thank you.

Mr. ROGERS. Thank you very much. I yield back.

Mr. DOYLE. The Chair now recognizes our first remote witness. Ms. Clarke, you are recognized for 5 minutes.

Ms. CLARKE. Thank you very much, Mr. Chairman, and let me thank our witnesses for participating and lending their expertise.

My question is for Mr. Johnson. In addition to having the privilege of serving on this committee, I also serve on the Homeland Security Committee as chair of the Cybersecurity Infrastructure Protection and Innovation Subcommittee.

During the decade and a half that I have served in Congress, I have observed malicious cyber activity grow more sophisticated and more frequent. An effective defense requires a full-court press, and there are appropriate roles and responsibilities for agencies across the Federal enterprise.

To defend critical infrastructure, PPD21 directs the Secretary of Homeland Security to coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure in partnership with sector risk management agencies which have more subject matter expertise.

I want to make sure that the legislation we are considering today supports that important model because it prevents silos and stovepiping.

Can you weigh in on the value of both DHS as a central coordinator for critical infrastructure protection and on the importance of sector risk management agencies? How should Congress continue

to develop those roles and to assure that the full capabilities of the Federal enterprise are more effectively brought to bear to defend our critical infrastructure?

Mr. JOHNSON. Thank you, Congresswoman, and that is—and I also honor your service on the Homeland Security Committee. You have been a great leader on these issues for many years, and I think that is a core question.

Just to lay out the PPD21 process, DHS and now through CISA is what is called the sector-specific agency for the communications sector. It is also the sector-specific agency for the IT sector. And similar to how the Treasury Department is a sector-specific agency for financial services, it is not a regulator.

The regulator in the space, in the communications sector is, of course, the FCC. There is not really a regulator for the IT sector except to the extent that some of the IT sector's work feeds into the communication sector through enforcement actions at the FTC. So that sector-specific agency, DHS and FCC relationship, is absolutely crucial.

And I know from my time at the FCC that a regulatory agency can either be a great enabler of that partnership, both between the sector-specific agency and the regulator and between the Government and industry, or it can altogether block it. And I think to answer Congresswoman Clarke's question directly, it is crucial to have that sector-specific agency regulator and then contributing agencies like Commerce. I have mentioned NIS and NTIA and even ITA and BIS. It is crucial to have those relationships crystallized, clear, everybody knows what everybody is doing, and maybe as importantly, everybody knows what certain folks are not supposed to be doing so that—and it is not about lanes. It is about a team.

So I think—forgive the football metaphor, but football season is approaching. Every position needs to know its unique role and unique value add and work together. And I think it starts with the sector-specific agency, but it also includes the FCC and the Commerce Department as well as others like FBI and other IC elements.

Ms. CLARKE. Very well. Well, let me be the first to yield back major time, Mr. Chairman. I yield back.

Mr. DOYLE. I thank the gentlelady.

Oh. Mr. Scalise has joined us, and Steve, you are up next. You have 5 minutes.

Mr. SCALISE. Well, thank you, Mr. Chairman, and good to be back in the committee in person, as well as Ranking Member Latta. I appreciate you having today's hearing and bringing up the piece of legislation that I drafted along with Congresswoman Eshoo, and I know she is here as well. I want to thank Congresswoman Eshoo on partnering with me on this important piece of legislation.

Our bill, H.R. 3919, which is the Securing Equipment Act, stops the threat of China from infiltrating our networks by prohibiting the FCC from issuing equipment licenses to Chinese companies that are identified as national security threats—not all companies, but companies that have made that distinction that the FBI or the FCC has now identified as national security threats.

In 2019, our committee worked in a bipartisan manner to help address the threat of China by passing the Secure Entrusted Communications Network Act of 2019. That landmark act instructed the FCC to do a few things; among those, publish a list of telecommunication equipment deemed to be a national security threat, prohibit the use of Federal funds for purchasing equipment made by those companies, authorize funding for U.S. carriers to rip and replace equipment that was made by those companies.

So earlier this year, the FCC did what they were instructed to do, and they, in fact, published this list. This is the first list that has come out. It lists five different companies that are on this national security threat list. Every company on this list has ties to the Chinese Communist Party with the Chinese Government having ownership in many of them. Clearly, you can see why that was a concern that the FCC identified. We also know all too well that the CCP wastes no opportunity to expose our vulnerabilities and to undermine our national security.

While the 2019 law took a major step in getting compromised tech out of U.S. networks, U.S. carriers can still provide privately purchased equipment from these listed companies on the open market, so these companies can still sell to American companies where that data can be controlled by the Chinese Communist Party. Since all of those companies are subject to Chinese national security laws, at any point the Chinese Government can choose to exploit them for espionage, tapping into their access in U.S. networks to gain critical information on individuals and sensitive government information.

As we expand our 5G networks and heavy data flows and the critical technologies that rely on these networks such as driverless cars and the Internet of Things, any existence of compromised technology poses a grave threat to our national security. Our bill seeks to further improve on the 2019 law. By prohibiting the FCC from issuing any equipment license to these companies, our bill adds an extra layer of security and puts a full stop to Chinese equipment from these threatening companies that are threats to our network. I look forward to having a full markup on this bill and moving it to the floor so we can better protect our networks.

And I also want to ask, Mr. Chairman. I will start with you, Mr. Johnson. As we look at the 2019 law that, among other things, directed the FCC to create this list which they now have done, these companies have had to do some things that are very, very alarming to be included on this national security threat list.

When you look at this proposed legislation by myself and Congresswoman Eshoo, do you think this gives an extra layer of protection to the FCC as we know lawsuits are going to come, as lawsuits have come by companies from other protective measures that our committee has passed so that the FCC has the ability to back up their actions, to back up this list by then following through and saying you are not going to be able to sell—companies that are threats are not going to be able to sell in the United States these jeopardized products?

Mr. JOHNSON. Thank you, Congressman. I really appreciate that question, and I think it has been noted the cognitive dissonance of the ban on Huawei and ZTE for subsidized U.S. networks, but the

legal availability of Huawei and ZTE everywhere else in the U.S. market has been noted.

Mr. SCALISE. And we see Huawei and ZTE challenging some of those laws as well.

Mr. JOHNSON. Of course. I will note the Fifth Circuit upheld the dismissal of the Huawei suit, I think last week, so probably on pretty solid legal ground as of now. Certainly, a statute backing up the FCC's authority would bolster that authority, and especially for something that is such—this is a very profound power that the FCC would have through this.

I love all my friends in the equipment authorization world, but it is a somewhat obscure radio frequency interference-based administrative law process. And so the power for the FCC to be able to block major companies altogether from the market is profound, and I think that underscores the importance of having fulsome processes from elsewhere in the Government that feed into those designations as has happened with the five companies that are mentioned first in the NDAA.

Mr. SCALISE. Thanks. I know we are out of time.

Mr. DOYLE. The gentleman's time has expired.

Mr. SCALISE. So hopefully by passing the Securing Equipment Act, we can address this problem and others.

And, again, thank you, Mr. Chairman, for allowing us to come up. I yield back.

Mr. DOYLE. Thank you. The gentleman yields back.

The Chair recognizes Mr. McEachin, who is joining us remotely. Yes. Five minutes.

Mr. MCEACHIN. Thank you, Mr. Chairman, and thank you for your very fine leadership in calling today's hearing.

Just to jump right onto it, Mr. Srihari, again, thank you for your appearance today. We have already had a little bit of a conversation about the creation of a 6G task force, which I think is crucial to helping the Federal Government meet the policy challenges that will come with future generations of wireless technology before they create a bottleneck.

Are there other things that we can do to make sure the U.S. leads the way domestically, and potentially, equally as important, internationally?

Mr. SRIHARI. Thank you very much, Congressman, for the question. So my colleagues have talked a little bit about the 6G issue and the legislation before you today on the 6G task force. When we talk about international activities, there is no doubt.

The Europeans have created a consortium, I think it is called Hexa-X, that is focused on the creation of 6G that is bringing together European industry stakeholders from the operator and vendor community, and they don't shy away from saying that the purpose there is to make Europe the global leader on 6G technology.

And, meanwhile, in 2019 China came forward with an announcement saying that they wanted to start an R&D initiative on 6G. And at the time, some people thought that that was really hyperbole and that it was too early, but nobody, I think, is questioning that now.

And while we do want industry to take leadership on these issues, I think having a coordinated public-private partnership ef-

fort that puts the U.S. in the game on 6G institutionally would be a good thing to do.

Mr. MCEACHIN. Thank you for that.

Mr. Boswell, for trusted suppliers, how do we leverage our international allies to ensure a diverse global market of trusted suppliers?

Mr. BOSWELL. I am sorry. Could you repeat that, please? It was a little hard——

Mr. MCEACHIN. I might even say it more succinctly. How do we leverage our international allies to ensure the diverse global market of trusted suppliers?

Mr. BOSWELL. It is important for us to work with U.S. allies and other representatives as it is a global marketplace that we are selling into in a global economy as well as from a technology perspective.

As we build out technology, it really—the scale that is involved there and the need to protect critical infrastructure is something that we are all facing. It is a global security issue, not just a domestic one. So we do have to continue to advance the adoption of different guidelines that enhance the protection of end users as well as the privacy of end users by deploying networks that rely on secure and trusted suppliers and a trusted supply chain, not just individual technologies or specific architecture type.

Being first in 5G for the U.S. is not only an economic award that we are striving for, it is also a meaningful step forward in national security. We must continue on that path with our allies.

Mr. MCEACHIN. Thank you for that.

Mr. Chairman, I am going to try to stay on your good side and yield back a whole batch of time.

Mr. DOYLE. Thank you, Mr. McEachin. The gentleman yields back.

The Chair recognizes Mr. Guthrie for 5 minutes.

Mr. GUTHRIE. Thank you, Mr. Chair. I appreciate the recognition.

And my first question is for Mr. Boswell. In our last hearing in April, we discussed the concept of open RAN. And we heard from witnesses about the challenge of integrating certain network components into their networks, particularly for smaller providers.

So my question is, what steps is Ericsson taking to work with small providers? And what role, if any, should Congress have in facilitating the deployment of open RAN compatible technologies?

Mr. BOSWELL. Small providers make up really the backbone of everything throughout the country. It is not just three, four, or five big carriers, right? It is everybody working together to build that connected network.

Ericsson has had a long history in this space. We serve over 150 rural and regional carriers across much of the U.S. Eighty percent of our customers in that space have been with us for over 10 years, so we have worked with them through that transition from 2G to 3G to 4G.

Some of them are just now getting to 4G and rolling out LTE, so moving towards 5G is a big deal for them.

Mr. GUTHRIE. What role should Congress have in this?

Mr. BOSWELL. Well, it is important to reinforce what groups like the CSRIC are able to do. We recently in some work in this most

recent CSRIC, in working group II, provided guidance specifically aimed at some of those smaller carriers that are going through a transition from 4G to 5G on what some best security practices are.

Mr. GUTHRIE. I do have a second part. I just want to make sure I get to my—and so it is kind of what our Republican leader asked, so maybe you can answer here or provide her the information that she asked, I guess.

But H.R. 432, which is the Open Outreach Act which creates the office at NTIA to provide technical assistance to small networks—so my question for you and then Mr. Srihari, if you will comment as well.

So first for Mr. Boswell: What guidance would you give to NTIA if it were to establish such a program and the scope of the legislation that may make the program more successful?

Mr. BOSWELL. Well, yes, I think so. There are pros and cons to any technology that we are trying to element, in particular, when we are talking about critical infrastructure where we really have to get it right all of the time. There could be increased complexities or life cycle challenges or even security issues that some of the smaller operators maybe aren't considering or were aware of.

So I am concerned that as it currently stands in the language, the bill focuses mainly on the benefits of open RAN, of which there are many. While Ericsson recognizes that these small providers may need more assistance than some of the larger carriers, government policy should really be technology neutral and not focused on any one technology type or architecture type.

Each particular provider should decide which technology is best for them without influence from the Government but also with the right amount of input and information in context.

Mr. GUTHRIE. Can I get Mr. Srihari? I have one got more question after this that I want to make sure I get to. So, Mr. Srihari.

Mr. SRIHARI. Yes. On the operator education, I would tell NTIA a few things. First of all, to lift up the stories of an operator like Inland Cellular in northwest Idaho and Washington, I think, that is already deploying it. I would introduce them to operators around the world that are deploying open RAN overseas already.

I would introduce them to systems integrators, including American companies, who are leading the way in open RAN network deployments around the world. I would do more things like the FCC operator showcase that they are holding in 2 weeks.

I would consider maybe pairing it with the C script program that educates small operators on untrusted vendors and getting that equipment out, and combine those programs. I think there is a lot they could do.

Mr. GUTHRIE. All right. Thanks. I want to get one more question, hopefully time for an answer. So now that Congress, Mr. Boswell, has appropriated funding for secure and trusted networks reimbursement programs, small and rural carriers are hard at work preparing to rip and replace untrusted gear from their networks.

But to keep these networks running is more of a rip than replace—more replace than rip. We have heard some about concerns for potential delays caused by permitting processes. I have H.R. 1053 to help the permitting process speed up by replacing equipment that poses a national security threat.

Mr. Boswell, would streamlining modifications of the existing infrastructure help promote the deployment of 5G and secure our networks?

Mr. BOSWELL. Yes is the answer.

Mr. GUTHRIE. He could have waited for 3 seconds.

Mr. BOSWELL. It absolutely would. No. There is many factors to consider there, but truly, we have to maintain the pace and not forestall deployments. Don't let perfect be the enemy of good.

Mr. GUTHRIE. It is already permitted. We are just replacing the equipment and so going through the permitting process.

Mr. BOSWELL. In some cases, that can add an additional 90 days to an application process. In a lot of different States, that process to review a simple antenna installation can be as arduous as a developer with a new building of an apartment complex.

Mr. GUTHRIE. Right.

Mr. BOSWELL. So we need some common sense to apply there.

Mr. GUTHRIE. Thank you, Mr. Chair.

Mr. DOYLE. The gentleman's time has expired.

The Chair recognizes the chairman of the full committee, Mr. Pallone, for 5 minutes.

Mr. PALLONE. Thank you, Chairman Doyle.

I wanted to start with Mr. Srihari. As you know, Congress has already been very active in supporting ways to make our wireless infrastructure and its supply chain more secure through the Secure and Trusted Networks Act and the USA Telecommunications Act, which still needs funding.

But in your written testimony, you note that open architectures could reduce the global grip of Chinese firms on the market and provide other advantages to both large and small providers. Could you explain what some of those advantages might be, if you will.

Mr. SRIHARI. Sure. Thank you for the question, Mr. Chairman. I would begin with greater flexibility. You avoid the problem of vendor lock in if you are an operator, especially a small operator, from being locked into one particular vendor.

You also get more flexibility in terms of where you house network functions out on the edge, on the towers, or in the core of your network. Also lower costs.

We have seen evidence that open RAN deployments can be more cost effective than traditional deployments. The gradual upgradability over time—software-based upgrading rather than hardware rip and replacements—that can lower costs. New innovation, new technology through artificial intelligence and machine learnings do things like automated threat detection.

Stronger security, energy efficiency. There are a number of these kind of technical benefits as we think about networks not just as a box that you deploy every 10 years but switching to a software virtualized ecosystem that is going through a cycle of constant—continuous improvement and continuous development.

Mr. PALLONE. All right. Thanks.

Let me go to Mr. Boswell. You refer in your testimony to Ericsson's ongoing work in the FCC CSRIC and that Ericsson has been engaged across several working groups in the most iteration of CSRIC focused on the 5G security, and one of the bills we are considering today would make CSRIC permanent.

So do you have a view on why making CSRIC permanent could be good for industry and good for the country as a whole?

Mr. BOSWELL. Yes, I do. Actually, I have two comments. First, I would like to address Mr. Srihari's comments about some of the benefits there and just add some clarification that many of those benefits listed are not unique to an open RAN or even open system architecture.

3GPP has long been an open and interoperable system. And, furthermore, from a software development or software upgradability standpoint, when Ericsson rolled out radios, tens of thousands of radios across the U.S. as long as 5 years ago, those have been upgradable to 5G with over-the-air software updates since we put them in, so much of that is not unique.

My time on CSRIC has been very well spent and very enjoyed, in particular with gentlemen like Faruq at Qualcomm. I very much enjoyed working with him in the past. I have firsthand knowledge of the importance of the work that CSRIC does. And this bill that you have talked about, it recognizes the significance of that task.

And in some cases, it is bleeding-edge or cutting-edge things that we are doing for new roles like network slicing or 5G standalone networks or how to enhance E911, and those are great. That is new best practices for cutting-edge things.

But we also, as I mentioned before, we have taken a look at things like, well, how can we help smaller operators that are transitioning from 4G to 5G. This is a big leap. It is a completely different kind of architecture. It is a software-based infrastructure.

For many of them, it is just a brand new world. And so one of the working groups specifically this past CSRIC looked at how to secure that transition to keep them secure throughout that process. So we really look at both ends of it.

I think it is very important to formally codify and recognize the work that CSRIC does.

Mr. PALLONE. Thank you.

And then, Mr. Brenner, you write in your testimony about the Emergency Broadband Benefit, which will provide discounted connectivity and equipment to about 3 million low-income households, and the Emergency Connectivity Fund, which provides devices and connectivity to millions of K through 12 students, and I am very proud of that work.

But in light of what I hope will be millions of devices getting to kids and families across the country very shortly, can you explain why it is important to make sure that those devices come from trusted vendors and describe how the Government and industry can work together to make that happen, to ensure that?

Mr. BRENNER. Sure. Thanks very much for the question, and I am very excited about both the ECF and the EBB programs. In addition to giving a shoutout to this subcommittee for the programs, Acting Chair Jessica Rosenworcel over at the FCC has done a tremendous job of not only meeting the deadlines but forging bipartisan consensus on the rules for both of the programs and then having this hugely successful rollout.

The short answer to your question, Chairman Pallone, is, you know, devices that have a Qualcomm chip inside, whether it is a smart—whether it is, in this case, a laptop, a tablet, a fixed wire-

less device, a modem, or a router, we spend a fortune to ensure that our devices that have our chip inside are secure, are reliable, can be trusted.

We work with every device manufacturer in the world to make sure that—to constantly test. When there are issues spotted, we, you know, pounce on them immediately. So it is obviously crucial for these programs to be successful.

And I think, you know, we would like to see for sure and hopefully for these programs, you know, to become permanent, that the devices be absolutely reliable and secure, and I have every confidence that that is happening.

Mr. DOYLE. The gentleman's time has expired.

The Chair now recognizes Mr. Kinzinger for 5 minutes.

Mr. KINZINGER. Thank you, Mr. Chairman. I thank our witnesses for being here. Appreciate it.

Over the past few months, we have seen rampant cyber attacks that have disrupted businesses, increased consumer cost, and threatened our national security. Cyber attacks are on the rise here in the United States, and since the pandemic, attacks have increased dramatically. In fact, a cyber attack happens every 39 seconds.

Perhaps an even more shocking statistic is that 95 percent of cybersecurity attacks are due to human error. As cyber crime becomes a growing threat in a post-pandemic world that is becoming increasingly more digitalized, businesses and the public alike need to be prepared. That is why I introduced H.R. 4055, the American Cybersecurity Literacy Act, with multiple colleagues on this committee.

This bipartisan bill would require the NTIA to establish a cyber literacy campaign to help promote understanding of how to stay safe online and prevent successful cyber attacks. This campaign will include lessons on how to identify malicious phishing emails, the need to change passwords often and use multi-factor authentication on sensitive accounts, and highlight cyber risk posed by the use of publicly available WiFi hotspots, among other issues.

I believe commonsense legislation like this bill that promotes cyber awareness and education are critical steps as we gear up to fight back against cyber crime.

Mr. Johnson, I want to ask you. Much of the legislation we are considering today is focused on cybersecurity. For example, H.R. 4046, the NTIA Policy and Cybersecurity Coordination Act, introduced by Representatives Duncan and Wild, would codify NTIA's cybersecurity office and require it to coordinate and develop policy regarding the cybersecurity of our communications networks.

Further, H.R. 4055 introduced by myself, Representative Eshoo, Representative Veasey, and Representative Houlahan would require NTIA to develop and conduct a cybersecurity literacy campaign to educate U.S. individuals and businesses about common cybersecurity risks and practices.

How would these additional tools build on NTIA's existing work in cybersecurity, is it an appropriate agency to administer these functions, and are there any additional tools we should consider?

Mr. JOHNSON. Thank you, Congressman. That is a great question and a very important issue, I think, especially following the Colo-

nial Pipeline attack. Not that any government initiative, literacy initiative could have prevented that, but just the fact of gas price spikes and cars lined up to get gas, for instance, in my home State in Georgia, it brought it home to voters and consumers in a way probably no other cyber attack ever has. So I think there is a greater awareness among people and businesses.

NTIA certainly has—and Commerce, more broadly, but NTIA in particular—certainly has an important role in this. As I was saying earlier, the Commerce Department—and often represented by NTIA and interagency discussions—is the only agency in government that talks about cybersecurity from the standpoint of a thriving digital economy. So—and that goes from consumers on devices to businesses in e-commerce and really throughout the economy.

And so promoting economic development and business innovation is at the core of what NTIA does, so they have a value. They have a valuable perspective to add on anything that has to do with how consumers and businesses should operate.

The only thing I would add is that DHS has done quite a bit of work on this as well, and so has the FTC. In my view, just to hit the drumbeat again, the core—we just need to have a coordinated full-court press, I think, as Representative Clarke put it. NTIA should be part of that. It should not replicate or it should not duplicate, rather, other parallel efforts and certainly shouldn't conflict, but NTIA, that is a lean, mean, fighting machine, as Dileep mentioned. They have a lot to offer, and they have a unique perspective.

Mr. KINZINGER. Let me ask you too. We have made strides in removing untrusted equipment in our networks, but there is a lot we need to do to secure 5G, especially with Internet of Things and software in the wake of the ransomware attacks, SolarWinds, Colonial.

We need a strategy to protect that infrastructure. What should Congress be doing to ensure we stay ahead of our adversaries when it comes to preventing those?

Mr. JOHNSON. I addressed this in my opening testimony. I think the core thing—and Congress has done this and should continue to do—it is promote an industry-led partnership with government. These network operators and their trusted suppliers have been doing this as a core business imperative for decades, and they are the core. They are the indispensable element of defending our country.

Mr. KINZINGER. Thank you. I have others I will submit, but I will yield back, Mr. Chairman.

Mr. DOYLE. OK. The Chair recognizes Mr. Veasey for 5 minutes, joining us remotely.

Mr. VEASEY. Mr. Chairman, thank you very much, and I want to thank the witnesses for being here today.

Obviously, security breaches are occurring more and more in the United States, and we need to make sure companies and our Government are doing everything that we can to protect citizens, but it is also important to give America a better understanding of how they can properly protect themselves online.

I am proud to have my bipartisan bill, the American Cybersecurity Literacy Act, which will provide Federal resources to educate

constituents on how to do everything from properly identifying secure websites to knowing about the potential cyber risks of using publicly available WiFi networks. Ensuring that all Americans have tools to protect themselves against harmful cyber attacks makes all of us safer in the long run.

Mr. Johnson, I know you had a wide array of experience here, so I wanted to ask you: Do you have a sense on where the public is in general on the cybersecurity awareness?

Mr. JOHNSON. As I just spoke with Congressman Kinzinger, I think there is a lot more awareness after the Colonial Pipeline attack than there was before in terms of cybersecurity being a day-to-day consumer and, frankly, voter issue. We have a long way to go, and I think the key is to making these steps concrete.

The problem with cybersecurity is it is all abstract, and if you are not a computer scientist it is hard to understand how these 1's and 0's could affect your life. So I think it is a matter of making simple—cyber hygiene is a term that is often used.

These simple steps like multifactor authentication make it clear to consumers and citizens what they need to do to secure their devices and their networks, and they will learn how to do it.

Mr. VEASEY. So, you know, that brings me to the next question I want to ask you. What sort of awareness, or not awareness, but do you have—do you or anyone else on the panel, for that matter, just have a sort of a basic understanding of how prepared the public is to protect themselves against cyber attacks?

Are there any statistics out there that shows what percentage of Americans are actually, you know, sufficiently prepared to truly protect themselves and understand all the risks and dangers out there? And, again, anyone on the panel can answer.

Mr. JOHNSON. I will just say there are a number of polls and studies like that. I don't think there is any one single answer because of the nature of the questions——

Mr. VEASEY. Yes.

Mr. JOHNSON [continuing]. That would need to be asked. Maybe a different indicator that might help get us there is the role that CEO—that C-suite executives and boards, their awareness and their activity on cybersecurity has dramatically increased in recent years.

And so I can get you specific numbers on that, but that may be a leading indicator as to how everyday consumers are increasingly prepared. But we have a long way to go, I think, on both matters.

Mr. VEASEY. No. Absolutely.

Anyone else have any thoughts on that?

Mr. BOSWELL. Sure. This is Jason from Ericsson. I will comment on that. As the proud father of a 9-year-old daughter, I am sure she would tell you that she is more than capable and deserves a cell phone and wants to be online more and more, but if she is watching, the answer is still no. It is a mutual responsibility to have an awareness of being online and knowing how to conduct business.

These used to be the kinds of things that we would teach our children when we taught them how to write a check in a checkbook or have responsible fiscal duties at home. That extends into now responsible activity online. But, frankly, I'm not sure that we have

ever faced such a convergence of this technology opportunity that we have heard about today with potential critical impacts.

I have been in this business for several decades and was around for the Mirai botnet attack, the Target breach, of course, SolarWinds which now has brought a lot of visibility to it, but those impacts are really measured in terms of loss of dollars and lost time and lost information.

Compromising the future is going to lead to loss of essential services or national assets or even loss of life, so it is up to companies like ours to get it right for the American people.

Mr. DOYLE. OK. The gentleman's time has expired.

And the Chair now recognizes my fellow Pittsburgh Pirate fan—but that only still gets you 5 minutes, Gus. You are recognized.

Mr. BILIRAKIS. OK. We never give up, and the Bucs are going to be good next year. That is for sure.

Almost since its inception—I want to thank the witnesses as well—there have been concerns about the cybersecurity and privacy risks associated with the TikTok and other Chinese-owned apps. A recent article titled "TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance."

It highlighted stories from former TikTok employees about China's control over the company's operations as well as information usage. These former employees mentioned that there existed a userwide list that detailed likes and hashtag uses.

Additionally, cybersecurity experts warn that TikTok's level of information collection creates risk of propaganda spreading to influence American app users as well as potential blackmail for young users who will grow up to be America's future leaders.

A foreign power with this much individualized access is a scary thing, indeed, in my opinion.

So, Mr. Johnson, with this backdrop in mind, approximately 41 percent of TikTok users are between the ages of 16 and 24. To your understanding, how knowledgeable are our young people that all of their actions as TikTok users are being cataloged by China and will potentially be used against them as they mature? And I know this is a very serious issue. If you could respond, I would appreciate it.

Mr. JOHNSON. Thank you, Congressman. Also as a father of an 11-year-old and an 8-year-old and a 2-year-old who is a long way away from this, I am also very concerned about that, about data collection from apps in general, but particularly TikTok for the reasons that you have outlined.

In the worst-case scenario, TikTok could be developing not just individualized, you know, portfolios of individual people but an aggregate big data set of I think 100 million Americans that could be used for all sorts of nefarious purposes, including—well, I will stay away from the intelligence capabilities, but the bottom line, I am also very worried about that, very concerned about that as well.

Mr. BILIRAKIS. Thank you. These concerns from TikTok whistleblowers proves the point we need a literacy campaign to educate the public on cybersecurity risks which should include the dangers of adversarial countries, their data collection and intentions.

So, H.R. 4055—actually, the main sponsor is my friend, Mr. Kinzinger, but I am on there as a colleague along with others, Representative Eshoo and others—but it would provide the needed

public literacy by establishing a consumer-facing campaign about common steps that will improve awareness of potential risks and hacks. We could spend a lot of time and money keeping Chinese equipment out of our communication networks, but if users are unwittingly sharing information with our adversaries through their devices, we are not closing the loopholes, in my opinion.

So the question again for Mr. Johnson: How would this bill, this particular bill—and I know you have reviewed it—help improve the security of our networks?

Mr. JOHNSON. And just to echo what I said to your colleague, I think the biggest value add is having the commercial business digital economy perspective that Congress and NTIA offers on these issues and recognizing that there are a hundred million Americans who want to use apps like this, like TikTok and others.

That is a reality that we have to deal with and have to hopefully leverage in order to promote security awareness, particularly among these young—our young people.

Mr. BILIRAKIS. I want to make a point. I hope my kids are listening as well. Thank you, and I yield back the rest of my time. Thank you, Mr. Chairman. Appreciate it. Go Bucs.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Soto for 5 minutes.

Mr. SOTO. Thank you so much, Chairman, and what an important topic we are talking about today, something that is sort of the battlefront of the 21st century when we think about SolarWinds, Colonial Pipeline, JBS.

We keep on seeing stories over and over, right, of breaches both in the highest levels of government and in some of the most sophisticated companies that we have in the United States, and it shows that we have to evolve. And, Chairman, I want to applaud you because when I look at the list of bills today, and they are very much bipartisan.

I know we find ourselves debating all these different issues, but this is something we are united on, that we have to step up our cybersecurity and that we have to protect our infrastructure from the threats, primarily abroad, that we're seeing.

Right now, we are debating a bipartisan infrastructure package, the American Jobs Plan, and we saw a bipartisan breakthrough. And part of building back better, part of the American Jobs Plan, is more than just the physical infrastructure. It is the technological infrastructure. It is making sure that we are bringing certain industries back home that are critical to our national security like telecommunications.

In central Florida, we are making microchips and we are making semiconductors, and we know with telecommunications there is going to be more and more of a push to bring both that, pharmaceuticals, personal protective equipment—we have always done it for defense—but some of these areas that are critical back.

We also saw the President go to the G7 and to visit with our allies at NATO, followed by an anticipated meeting with President Putin. And we know Russia continues to harbor a lot of these cyber terrorists.

And while we have to be aggressive on our foreign policy side, in a proportionate way, we also can do better to make sure our pri-

vate sector and government is ready back at home. And that is what we are talking about here today, making sure that we are using best practices, making sure that we get notice when folks have ended up getting hacked.

And I would like to hear from Mr. Johnson. Over the last year, we have seen an unprecedented growth with RAN ecosystem thanks to open RAN architecture, a technology that will allow us to go beyond a lot of the equipment we currently buy from China.

For example, Rakuten Network's announcement in Japan of a multivendor open RAN network, one of those vendors in the partnership is Airspan Networks, based in my home State of Florida. How important is it to develop and fund American-based vendors knowing what comes with that is an increase in high-skill jobs and the flexibility for a wireless network to adapt to the growing demands of a 5G network?

Mr. JOHNSON. Thank you, Congressman. And another crucial question for this moment. And just in full disclosure, one of my roles in private practice is I am outside counsel for the Open RAN Policy Coalition, and Airspan is a member.

And I will say that it is crucial to invest in companies like Airspan, not just American companies but trusted suppliers.

And here it is—I think the aperture that we should be looking through is certainly U.S.-based companies with operations and facilities and jobs in the United States but also companies that are organized and have operations in allied or partner countries.

And this is something that, to give to your G7 and NATO point, the scale of that market is what allows us to compete, you know, the free market democracies against authoritarian regimes.

And I think—I am not speaking for Airspan in particular, but my guess is they want to have a global market to sell to as well.

And so leveraging the dynamism and notification of U.S. and partner—of companies based in the United States and other rule-of-law-based market democracies, our allies and partners, is, I think, the crucial competitive edge that we have in the coming decades.

Mr. SOTO. Well, thank you, Mr. Johnson. We know many of these technologies we developed, right. Florida was a big part of developing the cell phone.

Right here in Virginia, they helped develop the rudimentary beginnings of the internet, and yet we saw through business deals a lot of the technology start being built abroad because it was cheaper. But we see now that has set us up for vulnerabilities, and today we are taking a huge step in making sure we build back better and to secure our networks.

And I yield back.

Mr. DOYLE. The gentleman yields back.

The Chair recognizes Mr. Johnson for 5 minutes.

Mr. JOHNSON OF OHIO. Well, thank you, Mr. Chairman.

And, Mr. Johnson, for you, starting out, you know, while we understand the risk that Huawei possessed to our networks and have acted to prevent its use domestically, there are other providers that could pose a risk to national security that may seek to enter the market as well.

Currently, the FCC authorizes approvals for foreign-controlled companies to provide services in the U.S., but they defer to executive branch recommendations on their national security review of the transaction.

As I mentioned, my bill would formalize this process while preserving the subject matter expertise of national security agencies.

So, in your view, Mr. Johnson, how does NTIA's expertise with interagency policy, development, and coordination suit them for being a single point of contact between the interagency, the FCC, and applicants? How important is it to ensure timely review of these applications?

Mr. JOHNSON. Thanks, Congressman. Let me just start with the caveat that there are many experts on TEAM TELECOM law, and that is not my area of particular expertise. But I think that the policy that has developed over the past couple of years—I get the timing mixed up because of the COVID time warp—but I think the Executive order that came out of the Trump administration formally organizing TEAM TELECOM and the agencies involved did help clarify roles in what had previously been more of an opaque process, and so I——

Mr. JOHNSON OF OHIO. And that is essentially what this bill does. It codifies that Executive order.

Mr. JOHNSON. Right. Right. And to answer your question about NTIA, and I think they are, NTIA and the Commerce Department, more broadly, and I know this from being—from previously working in the Commerce Department on these issues.

They are a crucial part of the process because, as I have said a couple of times today, they are the only agency whose core mission is promoting American business and innovation, which underlies American strength and security.

So you have the other security agencies who also have, obviously, a crucial role to play in TEAM TELECOM as well. They are coming at it from a purely security-oriented angle, and what Commerce adds is understanding the digital economy and the telecommunications economy.

Mr. JOHNSON OF OHIO. OK. Well, thank you.

For all of our witnesses, I am also pleased to be a colead on H.R. 4045, the Future Networks Act, along with my colleague Chairman Doyle. As you have heard, this legislation would create a 6G task force at the FCC to examine private-sector efforts regarding the development of 6G standards.

If you were a member of this task force—just very quickly, each of you—what advice would you have for Congress as we review this work? Starting with Mr. Srihari.

Mr. SRIHARI. Well, it is time to get started. The Chinese are doing it.

Mr. JOHNSON OF OHIO. Yes.

Mr. SRIHARI. The Europeans are doing it. So I think you take the approach that we want industry to lead, but we have to start looking at, you know, early on what are the new technology needs going to be, what are the use cases going to be, how can we leverage what American companies are already doing in terms of global standards participation.

Mr. JOHNSON OF OHIO. OK. Mr. Boswell.

Mr. BOSWELL. I mentioned earlier about the work that Ericsson has been doing with the National Science Foundation's RINGS program, which we are a founding member of as well as the platform for advanced wireless research. So we have gotten started here, but it is also important to make sure that we don't leave out the academia segment here. America's universities can provide a lot of input.

We have current partnerships that we have in place with the WINLAB at Rutgers, for example, with MIT, U.C. Berkeley, Stanford, NYU. I could list dozens more, but the university tie-in with some of these different efforts really allows them to, A, tap into some government funding, and then, B, also work with some of the industry experts that are actually out there building the networks. It creates a good cohesion and builds up our workforce in a place where we desperately need it.

Mr. JOHNSON OF OHIO. OK. Mr. Brenner.

Mr. BRENNER. So the private sector, led by Qualcomm, the American champion, we are going to invent 6G. We are going to drive the 6G technology. But where the Government and the task force can come in is, A, we are going to have to identify and free up spectrum for 6G. That is always a multiyear effort, number one.

And, number two, we are going to need to put these cell sites in places, and so the task force can work through site issues. And, by the way, for Mr. Soto, Airspan, fantastic partner of Qualcomm's. We make those chips for their small cells.

Mr. JOHNSON OF OHIO. OK. Mr. Johnson.

Mr. JOHNSON. I don't have much to add to my colleagues here, but I think that is the role of government, and therefore the role of Congress setting that up is to corral and harness this innovation that is taking place in the private sector and, as Mr. Boswell mentioned, in universities.

Mr. DOYLE. The gentleman's time has expired.

Mr. JOHNSON OF OHIO. Mr. Chairman, I yield back, but I do have some additional questions that I will submit for the record.

Mr. DOYLE. You can submit them. Yes. Thank you.

Let's see. Next up is Mr. O'Halleran, joining us remotely. Tom, you have 5 minutes.

Mr. O'HALLERAN. Thank you Mr. Chairman, Ranking Member Latta, for this opportunity.

You know, first of all, I have been listening to this for a while now, and I keep hearing things like, well, the pipeline issue brought this cybersecurity issue to a new level. I don't—this has been at a level, a high level, for as long as I can remember. We have been talking about security for businesses, for our Defense Department, and to get these networks up and going.

But here we are, running behind others to get this addressed. It is just amazing to me. And I know our chairman and our ranking member are trying as hard as they can. Securing America's network technology is an important national security priority. I am glad this subcommittee remains focused on this issue.

When it comes to expanding our networks, we have a lot of work to do, especially in rural areas and on Tribal lands. In my district, many households have no at-home internet access. This results in poorer health and educational opportunities for these families. And

we have miles and miles of dead zones where our cell phones read "no service." This is a problem when my constituents need to contact medical help or emergency services in remote areas.

We need to expand our network capabilities and those of the digital divide, and we must ensure that these networks are secure. This is not just a problem for large tech companies. Any hole in the network security can be exploited by hostile actors.

That is why last week I joined a bipartisan group to introduce the Open RAN Outreach Act. Our bill directs NTIA to provide outreach and assistance to small network providers to educate them on how to secure their networks using open network technology.

By helping small providers buying their components from trusted vendors, we can help secure the entire network. Small network providers, especially those in rural areas, cannot be left behind.

Mr. Srihari, you mentioned in your testimony the importance of raising awareness of open RAN among rural operations. What steps would you like to see Congress take to make sure that rural areas aren't left behind in the network security?

Mr. SRIHARI. Thank you, Congressman, for the question. One of the ironies of the rollout of open RAN around the world is that rural and smaller operators are in some ways actually leading the charge.

We see this largely outside the United States in smaller, unserved areas with new Greenfield deployments where there is no service before. You see operators coming in and doing open RAN implementations, and we see results with significantly lower costs and better performance in these areas.

So, as I mentioned earlier, I think it is just a question of making sure that small and rural operators know what is available to them today. There are American systems integrators who will bring the hardware and software together for them to make sure that they know what is available.

There is, you know, at least one operator in the United States, a small operator, that is already doing it, and a larger U.S. company is announcing plans for a nationwide network as well. I think it is just a question of making sure that these operators are connected with the information that they need, and I think the legislation would go a long way towards doing that.

Mr. O'HALLERAN. Thank you.

Mr. Brenner, how is Qualcomm supporting open network standards? And how would it help speed the development of 5G in rural America?

Mr. BRENNER. Oh, thanks very much for that question, Congressman.

We are absolutely pushing as hard as possible to develop chips that will go right into the equipment that will make open RAN go. We are working in every conceivable standards body to push for standardization of open RAN. As I said in my testimony, just a couple of days ago we announced a new small—the world's first 5G small cell open RAN platform that has the latest 5G technology in it. We are working with everyone and, you know, we think it is great technology.

And I also want to put a plug in for our fixed wireless technology. So while it is true——

Mr. O'HALLERAN. Mr. Brenner, I am sorry. I only have 15 seconds, and I want to make a quick statement.

Mr. BRENNER. OK. Sorry.

Mr. O'HALLERAN. No, no, not your fault.

I just—I don't want America to be behind other countries, and we have to do a process here that gets us further ahead, not just catching up. We need to get this done.

And so I yield, Mr. Chairman.

Mr. DOYLE. The gentleman's time has expired.

The Chair now recognizes Mr. Walberg for 5 minutes.

Mr. WALBERG. Thank you, Mr. Chairman.

And thanks to the panel for being here. I come in here thinking I am starting to understand everything about what we are talking about, then I realize, after listening to you, I got to keep working.

This year, the FCC announced its intent to recharter CSRIC to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of our Nation's communication systems. Last week, Representatives Slotkin, Schrader, and I introduced H.R. 4067, the Communications Security Advisory Act of 2021, which would simply make the council permanent.

Mr. Johnson, what is the best way to structure the council and define its focus, assisting the FCC as much as possible?

And, Mr. Boswell, I will ask you to follow up on that.

Mr. JOHNSON. Great. Thank you, Congressman, and appreciate the—your focus on CSRIC. I have to say I have—there is a special place in my heart for the CSRIC, despite its being possibly the worst acronym in a town of bad acronyms.

CSRIC is—it is really one of the crown jewels of our Government, I think. For those who don't know, it is the Communications Security, Reliability, Interoperability Council that advises the FCC. It is a collection of experts from industry, from government, and really throughout the ecosystem, to make sure that our 9–1–1 systems work well, that emergency alerts, that cutting-edge issues like 5G security, and I know both companies that are represented here today have advanced that significantly in recent years. I look forward to what this next CSRIC is going to do, focused on 5G issues.

I think the best way—and I do think there will be some value in statutorily backing up CSRIC. I think the—and I don't have any particular suggestions for revising your bill. I think it could really provide a long-term backing to a committee that—or a council that adds tremendous value.

And the only thing I would advise is to make sure that it remains flexible in terms of how each FCC puts it together. Because, for instance, there is a—you know, with the two attacks that have been so high profile in the past couple of months, there are elements of those—of each of those attacks that might be grappled with in CSRIC, and I think—so I think the flexibility is valuable.

Mr. WALBERG. OK. Flexibility. Mr. Boswell?

Mr. BOSWELL. I think from a U.S. perspective, you know, we have an obligation or a responsibility to the rest of the world to continue leading in 5G. CSRIC is one of the bodies that helps us do that. And by codifying it and showing the support behind it, I think it supports that on a global stage as well. I have been in-

volved in several CSRICs myself. And usually not too long after our reports get published, then I have colleagues from around the world that end up referencing those reports—"Well, the U.S. says that this is best practice, the U.S. says that this is best practice"—because they know we have the most secure and most reliable networks right here in the U.S.

So this puts kind of the pen to paper from the engineering standpoint of saying this is truly best practice, because this is what U.S. operators do. I think that is very important.

Mr. WALBERG. Do you think, Mr. Boswell, that recommendations of CSRIC should be mandatory, or should each company identify how best to incorporate their recommendations?

Mr. BOSWELL. I think that each company should identify how to best incorporate those recommendations, and we do take that into account as we work through each CSRIC on what is a best practice and what is a "this is a must have." There are certain recommendations in every CSRIC report that kind of stipulate, well, "this is for good security, you really have to do these certain things." For others, it is really dependent. Our operators have a good track record of taking a risk-based approach to the different layers that make up their network, and what makes sense in one region or architecture type may not necessarily make sense and even be a burden on them if forced to implement certain things.

Mr. WALBERG. OK. Mr. Brenner, I have a question to ask of you, but in the time here and with my chairman sitting behind me, I am going to have to direct it to you and get an answer to follow up. Thank you so much.

I yield back.

Mr. DOYLE. I thank the gentleman.

The Chair recognizes Miss Rice for 5 minutes.

Miss RICE. Thank you, Mr. Chairman.

Mr. Srihari, you started your comments by talking about NTIA and the FCC and their need to be able to execute all of their additional functions. What kind of an investment are we talking about from a monetary perspective?

You know, we can sit up here and say this is what all these different agencies are now tasked to do, but if we don't give them the resources to actually carry out those responsibilities, it is all for naught. So if you could just kind of put a—is it a dollar figure? A human capacity? What would you say?

Mr. SRIHARI. So six of the nine bills today, I think, would do something to NTIA or add some functions to NTIA. Most of them, I believe, would come under the budget category of—the umbrella category of domestic and international programs at NTIA. As of fiscal year 2020, there were 27 people who worked in that division. I think last year it went up into the 30s. I think President Biden is proposing to take it to 52.

So this is not a very large agency here. The whole agency, I think, has about 150 employees. I think the budget proposal this year is to add another $4 million, $5 million. And this is an agency that also does Federal spectrum transfers that yield the Government $100 billion. I mean, there is literally 1,000—10,000 times payoff for the Federal Government with this agency.

So I think, if this subcommittee rightfully is going to bolster NTIA's functions here, I think you need to be cheerleaders for the agency in very modest budget increases to just help them do these things. Right now, I am working with them on a number of different issues, and I see the same staffers' email being cc'd on three very different topics because they just don't have the people right now. That is the reality right now.

Miss RICE. Yes. Well, thank you for highlighting that.

Mr. Boswell, you mentioned in your opening remarks that Ericsson, even before the pandemic, put in place very tight controls on supply chains, and that set you up well. Can you just explain? Obviously, that is something that we as a Congress have to address, that our entire supply chain system just broke down under this pandemic, and we were left—you know, States were left playing Hunger Games to try to get PPE, et cetera. So can you just give—enlighten us, you know, as to how you put that—those controls in place?

Mr. BOSWELL. Sure. So, really, when we talk about solutions or building a network, there is kind of two categories. There is the hardware and the software side of it. Now, everyone says, well, all of the networks of the future, it is all software, but there is still hardware somewhere. It is not just sitting out there in space, right? So the hardware part is still very important.

We build that hardware on top of a trusted chipset where certificates, attestability and authenticity verification gets loaded at the factory level, at the chipset, so that we know it is a legitimate component that is out there in the field. That also allows us to, as there is software that is built on top of that, one level, attest to and kind of certifies or verifies the level above it. That is on the hardware side.

Software, it is really about good process, good software assurance. We have been best in class in this for a long time. Some of the recent legislation proposals that we have seen around software assurance are kind of heading other parts of the industry in the right direction there. But it is about doing things in each layer of it, not just saying "I have got a bill of materials" or "I have got a secure coding practice" or "I have got secure rollout." It is all of those processes.

So we have an end-to-end framework that starts with the developers, of course. They are the ones that write the code. But that goes all the way through until we are out there in the field, literally with the field tech on the side of a tower, connected to a baseband radio. They are still installing software there. So our processes cover that end to end from the moment it is on somebody's keyboard to the moment that it is up on a tower.

Miss RICE. Thank you, Mr. Boswell.

Mr. Johnson, you mentioned before the issue of territoriality. You know, some could accuse the way Congress is set up, these committees, we have—there is too much—too many committees that have too much jurisdiction over too many Federal agencies, and that really reduces the efficiency of those agencies. How can we make everyone work together better?

I mean, I know we learned a lot after 9/11, but this pandemic exposed that there are still those inefficiencies within these agen-

cies. What is your best piece of advice for us to, you know, to take going forward?

Mr. JOHNSON. As a former committee staffer on the Senate side, I don't have any answers for the congressional side of the jurisdiction. I will let you all work that out. But with regard to oversight and the executive branch, including independent regulatory agencies, I think simply demanding that they are working together and that they are part of the same team, as every committee's focus in oversight, will help make it happen.

I also think it has happened through the pandemic, because you had a lot of dedicated public servants working with a lot of companies to make—to keep us connected. And the FCC had a role, DHS had a role, and it—we are better than we were a year ago.

Mr. DOYLE. The gentlelady's time has expired.

Miss RICE. Thank you.

Mr. DOYLE. The Chair now recognizes Mr. Duncan for 5 minutes.

Mr. DUNCAN. Thank you, Mr. Chairman.

Mr. Boswell, that is a great goatee. I don't know who wears it better, you, me, or Gus Bilirakis. It has been a long hearing. I appreciate the levity there.

I want to thank most of you for your opening statements where you show some sort of support for H.R. 4046, the bipartisan NTIA Policy and Cybersecurity Coordination Act we have introduced with Ms. Wild and Mr. Curtis.

Small communications providers are a critical part of securing the domestic supply chain. That is why in the Secure and Trusted Communications Network Act, Congress took a bipartisan action to help smaller carriers remove untrusted equipment, and we have talked about that—I think Steve Scalise was big on that earlier—including by instructing NTIA to implement a program of—to guide small and rural providers when it comes to making better investments in equipment and services. This program entitled Communications Supply Chain Risk Information Partnership I think was established last summer.

To your knowledge has this program been successful? Any of you, all of you.

Mr. Boswell, you can start.

Mr. BOSWELL. I am not sure I can speak to the specific program that you are asking about. In regards to 4046, the current bill, I do think it makes sense to have an office at NTIA that is dedicated to these kinds of issues. We are particularly happy to see that this requires that an Associate Administrator with focus on market-based policies and promote innovation, competition, consumer access, digital inclusion, and economic growth—I think we would all agree those are good things. But all of that is consistent with the technology-neutral approach that Ericsson has long supported. We are very supportive of the bill also.

Mr. SRIHARI. I think they are just getting started with the C–SCRIP program, from what I have heard. I think they are planning on having some workshops in the near future. I don't know if they have actually started the engagement yet. This was set up by section 8 of the Secure Networks Act. But I do think the policy coordination office that your bill does, that is the office that would be handling this program, yes.

Mr. Brenner?

Mr. DUNCAN. Thank you so much.

Mr. BRENNER. Yes. I have the same understanding as Mr. Srihari that this is in an early stage. It is being rolled out.

You know, the only other thing I want to say is—I will harken back to something that Mr. Srihari said earlier, which is, you know, so spanning the prior administration and this one, you know, NTIA has had a lot of change in its leadership and we don't have a permanent leader right now, and you have all these bills, six of the nine bills, that make all these changes to NTIA. Some are minimal: write a report. Others, you know, changing the focus of an office and turning NTIA into having cyber as one of its core functions, that is a very significant change. And it is to going require, you know, a permanent Administrator to roll it out. And it would be good to get that person's views, I think, before Congress, you know—before legislation like that is signed into law.

Mr. DUNCAN. Mr. Johnson?

Mr. JOHNSON. And I will just mention that the present director of OPAD, the office here, is actually the Acting Administrator of NTIA, Evelyn Remaley. She is a good friend to many of us. She is an American treasure, I think. Doing a great—a great job with a small group of experts. And so I think colleagues are correct, the C–SCRIP program is just getting started, but I know from experience it could have a big impact.

A predecessor of it was what was referred to as the—a rural road show. In the past couple of years before the pandemic, DHS, NTIA, ODNI, and a number of other agencies traveled—went around the country to different—for different rural focus, small teleco-focused supply chain outreach, and it, in many ways, I think it helped pave the path to the rip-and-replace proceeding and—or transition, I should say.

And so the same people that were working on that for NTIA will be developing this program, and they are—they hit way above their weight, small office, but the good news is they can do a lot of good with hitting above their weight.

Mr. DUNCAN. Yes. Thank you for that.

Mr. Chairman, before I came to this committee, I was on Homeland, worked with Ms. Clarke and Pat Meehan and some others on cybersecurity issues. I am glad we are doing this, and I appreciate your support.

With that, I will yield back 12 seconds.

Mr. DOYLE. I thank the gentleman.

The Chair now yields 5 minutes to Ms. Eshoo remotely.

Ms. ESHOO. Chairman Doyle and Ranking Member Latta, thank you for this very important hearing today.

And to—I have been listening to the witnesses, what, at least 2 hours and 15 minutes, and I think that each one of you has done a superb job.

To Mr. Johnson, all of your background and previous experience really shows. But I want to point out something that maybe most colleagues don't know, and that is that Mr. Johnson is the son of a former colleague, a Member of the House, actually a classmate of mine. We entered the Congress together. So a warm welcome to you.

Mr. Johnson, in the last Congress, and it is—Mr. Scalise spoke of this—we passed legislation directing the FCC to ban telecommunications carriers using Federal funds to purchase equipment made by Huawei and other entities that posed a national security threat.

On this particular subject relative to Huawei, I have been like a dog with a bone. I served almost a decade on the House Intelligence Committee, and going back to 2009, 2010, I have been on this issue. I am pleased that we are making progress. So I want colleagues to know that this is not a newfound issue on my part.

Now, the legislation that we passed in the last Congress left a gap, because companies can still purchase equipment that poses national security threats using private funds. So Mr. Scalise and I recently introduced the Secure Equipment Act to close the gap. Our legislation prohibits the FCC from approving any equipment from Huawei [inaudible] international security threats, and this includes all privately purchased equipment.

Can you just briefly tell us about how having any vulnerable equipment in our networks poses risks to the entire network?

Mr. JOHNSON. Thank you, Congresswoman, and another really important question. And thanks for your leadership on these issues over all these years.

I think it is a—you know, there are many metaphors or analogies that you could use about the weakest—you know, the weakest link in the chain, or if one part of the network is compromised, it can affect the whole network. But just give two answers to that.

One is that with 5G—and I think Mr. Boswell could probably speak to this in some depth—the technical architecture of 5G actually can, I think, help us address that problem just as a matter of isolating threats. But that—in my personal view, that does not mitigate, sufficiently mitigate the risk of untrusted equipment like, again, in my opinion, Huawei and ZTE.

And so, if Congress has passed laws that ban Huawei and ZTE from Federal procurement and from being included in universal service fund subsidized networks, it does beg the question of what about its legal availability in all—in all other areas.

Ms. ESHOO. Uh-huh.

Mr. JOHNSON. So the bill that you and Mr. Scalise have put forward would close that gap, as you put it.

Ms. ESHOO. Great. Let me just get another question in.

I worry that we are not paying enough attention to threats to 2G, 3G, and 4G networks, even though most calls and texts and mobile data, you know, traverse these networks. There have been a lot of one-off reports. I think we need a comprehensive study on what vulnerabilities exist, what has been addressed, so that we the policymakers have a whole picture. Mr. Kinzinger and I have the Cybersecurity—the Understanding Cybersecurity of Mobile Networks Act. That requires the NTIA to study the issue.

As an expert, do you think that we are appropriately concerned about risks in the older networks?

Mr. JOHNSON. That is a great question. And the good news is there has been a lot of work done on that through CSRIC—on those issues through CSRIC at DHS. I think you are right that the focus in the past couple of years has been forward looking to 5G

and the transition to 4G—from 4G to 5G. But you are right. These 3G and 4G networks, and in some cases even 2G, will be—will be there for a while, and it could add some value to have a holistic look at those existing networks.

Mr. DOYLE. The gentlelady's time has expired.

Ms. ESHOO. Thank you.

Mr. DOYLE. The Chair now recognizes Mr. Curtis.

Mr. CURTIS. Thank you, Mr. Chairman.

Mr. Johnson, we talked about the cyber attacks a lot today. I want to go back to those. With the attacks, it is important to understand, if our Federal policies are effective and if the Federal roles and responsibilities are sufficiently coordinated. How do you see policies like the NTIA Policy and Cybersecurity Coordination Act better preparing us for these types of threats to our national security and boostering our influence abroad?

Mr. JOHNSON. Thank you, Congressman. I do think what it—what a bill like that would do is help galvanize the real advances that have been made in recent years, and including advances that have happened on the battlefield, so to speak, during the pandemic and through these recent high-profile attacks.

Mr. CURTIS. Another question. The Open RAN Alliance is an important step to establishing a global set of standards for governments and telecommunication providers to follow as we work to secure our networks from the Chinese influence. How many O–RAN networks are currently deployed to the United States, and what additional steps does the United States need to take to strengthen O–RAN standards to increase adoption domestically?

Mr. JOHNSON. I think—and thank you for that question as well. And as I mentioned earlier, I serve as outside counsel to the Open RAN Policy Coalition, which is sort of the policy counterpart to the O–RAN Alliance technical specifications work. There—Dish has announced that it is building a national network based on open RAN. As Mr. Srihari mentioned, there is a small provider, Inland Cellular, that has an open RAN network right now. But I think the—I think the way I would characterize it is we are presently, we the United States and also the world, are at an inflection point in developing and deploying open RAN solutions.

In my view, the role of the Government here is to do what it has been doing in promoting awareness, facilitating industries' innovation, and—because this is—the progress toward open networks in general and open RAN in particular is happening, and I think that is the—the role of the Government is to help facilitate that.

Mr. CURTIS. Great. Good. How can we work with our international partners to export this innovation and encourage our trusted vendors abroad?

Mr. JOHNSON. That is a very important question. And just to restate something I said earlier, I think the core of this is making clear that U.S. policy and U.S. national interests are shared among U.S. allies and partners. And so there is critically—you know, there is always a critical need for U.S.-based manufacturing and U.S. jobs, and also there is a core interest in trusted suppliers who are based in allies and partners, and also the ability for U.S.-based companies to sell, to export to those.

Mr. CURTIS. I wish I could give you more time. I am going to keep moving on.

Mr. Brenner, Mr. Boswell, your two companies are the largest 5G equipment manufacturers worldwide. Based on your industry experience, how do you anticipate China would respond to a policy like the Secure Equipment Act becoming law?

Mr. Brenner first.

Mr. BRENNER. Well, so I want to be clear on one thing which I don't think has been brought out yet, which is, you know, in parallel with your legislation, 2 weeks ago, the FCC issued the notice of proposed rulemaking that the legislation would require. So, you know, Congress, of course, is fully within their prerogatives to adopt the law, but the FCC is moving forward. You know, your law—your bill would set a 1-year deadline. FCC notices of proposed rulemakings don't have a deadline like that, but they are moving ahead.

As to, you know, how China writ large would react, the only thing I can say about that is, you know, China is extraordinarily important to Qualcomm. We are an American company. Every time someone in China buys a cell phone with a Qualcomm chip inside, that is real-life American leadership, and that is happening very, very much.

Mr. CURTIS. I am going to give Mr. Boswell a chance to respond.

I do want to point out, though, that what—congressional action means it can't be changed.

Mr. BRENNER. Right.

Mr. CURTIS. Right. So, Mr. Boswell.

Mr. BOSWELL. Well, I certainly can't speak for any government, foreign or domestic, and especially not the Chinese Government on what their prerogative would be. But from an outside layman's perspective, I would guess they may not be happy. But I am not a diplomat. I am an engineer. I build networks, I secure networks. That is what our mission is at Ericsson. So I will stick to that in my lane.

Mr. CURTIS. And, unfortunately, we are out of time. So we are going to have to rest on that.

Thank you, Mr. Chairman. I yield my time.

Mr. DOYLE. Thank you, Mr. Curtis. The gentleman yields back.

The Chair recognizes Ms. Matsui for 5 minutes. She is joining us remotely.

Ms. MATSUI. Thank you very much, Mr. Chairman, and thank you very much for this wonderful hearing. And I want to thank the witnesses for providing their expertise.

You know, I joined with Congressman McCaul to introduce the CHIPS Act, which would help address the semiconductor shortage by increasing American manufacturing capacity. And I included the CHIPS Act as an amendment to last years' NDAA and recently met with President Biden and NASA Security Advisor Sullivan about the urgent need to fund the programs authorized by this bill.

Now, given the meteoric rise of Chinese semiconductor manufacturing, I believe fully funding the semiconductor programs in the NDAA should be a top national security priority for this Congress. The Chinese are making significant investments, and the United States cannot afford to fall behind.

Mr. Brenner, is Qualcomm supportive of fully funding the CHIPS Act? And how would the bill help reestablish American leadership in this crucial 21st century supply chain?

Mr. Brenner? Hello?

Mr. DOYLE. Mr. Brenner, is your microphone on?

Mr. BRENNER. Yes. Sorry.

Mr. DOYLE. Thank you.

Mr. BRENNER. I am sorry about that.

Thank you for that question, Congresswoman Matsui. Qualcomm wholeheartedly supports the $52 billion in the CHIPS Act. And it is important to note that I think there is a lot of focus just on fabs for chips, on funding for that, but, you know, to build a domestic supply chain requires fabs, assembly, testing, advanced packaging, R&D. And all of that requires massive investment, and having the $52 billion weight of the Federal Government behind all of that would be a very good thing.

In addition, we are not waiting for it, though. One thing we can do is actually, through the standards process, we are working on supply chain security. That is another step that can be done, and Qualcomm has been a leader in that as well.

Ms. MATSUI. Well, that is great. Thank you.

To help secure telecommunication supply chains, we must work to ensure they are as diverse and reliable as possible. As an original cosponsor of the USA Telecommunications Act, I believe we need to fund the programs included in last year's defense bill to support the development and deployment for open RAN. The Senate-passed USICA appropriates $1.5 billion for the NTIA grant program and $500 million for the multilateral program. These are bipartisan figures, and I hope the House can keep pace.

Mr. Srihari, do you believe the funding authorized on the bill should serve as a floor rather than a ceiling, and how could additional funding help support American leadership in open RAN?

Mr. SRIHARI. Congresswoman, absolutely I think it should be viewed as a floor and not a ceiling. I think there is so much opportunity for the U.S. Government to be supporting the development of open RAN technologies, and not just open RAN, open network architectures, including Open Packet, Open Transport, Open Core, and the like. I think there is a big paradigm shift, as my colleagues here have talked about, that is coming in the next few years, and the more that Congress can do, I think the faster this transition will happen.

Ms. MATSUI. OK. Thank you.

Earlier this year, I wrote to President Biden urging him to develop a unified approach to spectrum policy, promoting cooperation, and establish a clear process for resolving interagency disputes. Moving forward, it is critical that NTIA resumes its role as manager of the Federal Government's use of spectrum and that agencies have transparent and consultative processes for freeing up needed spectrum.

As a case in point, I recently wrote to Acting Administrator Remaley, urging NTIA to work closely with DoD to facilitate a timely auction of the 3.45 gigahertz band.

Mr. Brenner, how do breakdowns in interagency process hinder our ability to meet our spectrum goals, and what role can the

Biden administration play in facilitating a more cogent spectrum strategy?

Mr. BRENNER. Well, thanks so much, Congresswoman Matsui. That is absolutely crucial. NTIA has that role, and they need to be given, you know, full authority from the administration. The administration so far has put a lot of emphasis on wireline broadband, which has certainly a role but, you know, everyone needs connectivity wherever they are, wherever they are going, and, you know, they need to do that. We need mobile connectivity. And the only way to resolve these spectrum issues is through close collaboration by NTIA as the single focal point for the Federal Government on the U.S. Government side and the FCC.

Ms. MATSUI. OK. Well, thank you very much.

And I yield back 1 second.

Mr. DOYLE. I thank the gentlelady.

The chairman recognizes Ms. Kelly for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair, for holding this legislative hearing. And thank to you the witnesses.

The Colonial Pipeline attack, which occurred due to cyber criminals gaining access to Colonial's operational technology network, reflects a fundamental paradox which has been exposed and magnified during the pandemic. On one hand, in the past year the increased use of online services has been invaluable in retaining personal connections and continuing business operations. But on the other hand, the increased use has exposed individuals and businesses to an unprecedented variety and volume of digital threats.

Mr. Johnson, can you tell how good network security and design practices can prevent cyber criminals from gaining or exploiting access to an organization's systems?

Mr. JOHNSON. Yes. Thank you, Congresswoman. And I think that is the—this is—the best way to look at this is that the sophisticated threats that we face, particularly from nation-state actors and intelligence services, but also from criminal groups that in many cases are affiliated with those nation-states, they are—they have the capacity to attack and affect most networks, most enterprises. And so the issue is making it harder for them and more costly for them to do so.

I am not expert on what Colonial Pipeline, how they were—how they were prepared, but it—I will just say I think that all of industry in most sectors need to step up their game. What I will—let's just go back to what I opened with, and I think this is really important. The communications and IT sectors, you know, that are the subject of your jurisdiction, they—their interests in—their private interests in network security reliability, cybersecurity, is essentially completely aligned with the U.S. Government's interests. That is not the same in other sectors. So if their network goes down, their business goes down, and this is what they—they provide, secure, reliable connectivity.

So I think there is a lot to learn. There is some other parallels in other sectors, like the financial sector, but there is a lot to learn from how the communications and IT sectors approach their work. And I think that there is a lot to build on there.

Ms. KELLY. OK. In Colonial's case, I know a single leaked password for an active account to the network allowed access to Colo-

nial's network. So while implemented networks and network security can block cyber criminals from accessing or alternating secure information, I am also concerned that when people think about cybersecurity, they get overwhelmed and confused by the amount of information and different approaches to cybersecurity. And, you know, I am going to say I am a little like that too. I am not an expert.

Mr. Boswell, how do you believe a cybersecurity literacy campaign like the one proposed in H.R. 4055 would help?

Mr. BOSWELL. I do think it is very important to increase, as I mentioned before, about the awareness of the American people of the impact that being online can have on their lives, that it is not just potentially a lost credit card or an inconvenience; that as technology pervades more and more into our society, that that impact itself could be a lot larger.

When cyber criminals are looking to exploit and attack, there's usually three things they are trying to do. It is either to get money, to get information, or to disrupt service, or, in some cases, all three. Those are generally their motivations. And so, when we think about it from a protecting-the-network perspective, it is easy to fall into the trap of you just say, "Well, f it is money they want, if I can just make it not profitable for an attacker, then I will be OK." Or if it is information, "Well, if I just protect my data while it is at rest and while it is moving across the network or while it is in storage, then I will be OK." Or if they want to disrupt services, "Well, if I just build out a cloud-based architecture, redundant services, high resiliency, then I will be OK."

The truth is we have to do all of those things all of the time to have a truly resilient network, and I think that holistic view is where we could increase education the most.

Ms. KELLY. I am going to get to Mr. Brenner. How do you monitor, map out the security of your supply chain, given your significance to the mobile industry? And I don't have a lot of time, so——

Mr. BRENNER. Yes. Well, constantly requires constant efforts, because, you know, it means the whole chain from beginning to end. So we have a team of people that works on our supply chain that are constantly, you know, monitoring and making—you know, taking every conceivable step to make sure that our supply chain is secure. And I am very happy to say that it is.

Mr. DOYLE. The gentlelady's time has expired.

Seeing no more Democrats, Mr. Joyce is waiving on. And we are pleased to have him here in the committee.

And you are recognized for 5 minutes.

Mr. JOYCE. Thank you, Chair Doyle and Ranking Member Latta, for allowing me to waive on to today's Communication and Technology Subcommittee hearing.

And to our witnesses, for a long morning, thank you, Mr. Srihari, Mr. Boswell, Mr. Brenner, Mr. Johnson, for being with us on this incredibly important discussion.

Today's conversation has been insightful. It is clear that we must empower the private sector to innovate at a rate necessary to stay ahead of cyber threats. The Federal Government must partner with these innovators to ensure that our Nation's networks and that our data are secure.

The human element is critical to this discussion as well. Efforts like those envisioned in H.R. 4055 and existing efforts by the private sector to increase cyber literacy and cyber awareness are also critical in defending our systems.

In fact, within my district, Gettysburg College and the cybersecurity company Fortinet established a partnership to modernize campus cybersecurity. Defending the network from nefarious actors, this partnership could serve as a potential model for cybersecurity throughout our country's ecosystem. Cybersecurity needs to be present in all areas: in education, business, in energy, in healthcare, in communications, and in national defense.

Mr. Johnson, do you believe that we need to extend an all-of the-above approach with strong public-private partnerships that innovate cyber solutions and make a cyber-aware population?

Mr. JOHNSON. Absolutely. It is crucial to our future. And I like your all-of-the-above. It needs to be a coordinated full-court press.

Mr. JOYCE. Mr. Brenner, do you see additional possibilities in this all-of-above approach? Do you see additional opportunities specifically in public-private partnerships?

Mr. BRENNER. Absolutely. I mean, we all the time engage with governments, all in the United States and all over the world, and we are always open to that kind of thing.

Mr. JOYCE. Mr. Boswell, can you add to this conversation?

Mr. BOSWELL. Yes. You know, we were talking earlier about some of the early 6G work that is going on with the National Science Foundation and PAWR which—forgive me—the Platforms for Advanced Wireless Research program. One of the things they are working on is working with industry experts like Ericsson and Qualcomm and many others, as well as Government agencies, so tie-ins from the NSF, from DoD, from other spaces, but then the academic spaces as well.

So they are working with NYU, Rutgers, Columbia, Salt Lake City, Utah, University of Utah, and Rice, NCSU, Mississippi State, Purdue, Iowa State. Sorry if I left out a university. There's a lot of them that this group is working with.

And I think that is really important, not only to make it that it is not just a conversation between those of us that have done this for a few decades on the policy side, on the protecting national infrastructure side, on the building equipment side, but also those that are coming in the next decade.

So working with these universities, we are identifying that is the next generation of the people that are going to be sitting here 20 years from now or—I don't know, maybe they will take our seats here sooner. Who knows, you know? But that kind of collaboration with the university system I think is really important to reestablishing American innovation.

Mr. JOYCE. Mr. Srihari, can you add to this conversation?

Mr. SRIHARI. I think your talk about public-private partnerships is an important one. Your Gettysburg example, for example, in your district.

I know the bill before us today talks about creating a national program at NTIA for cyber education, but the reality of the situation is that good cyber hygiene and best practices is about teaching kids in high school. It is about the local college working with the

students, or an employer teaching its new hires the basics about good cybersecurity. It is these basic sort of private-sector partnerships maybe with the local government, the State government, the local mayor's office. That is where the first line of defense is on cybersecurity, and I think you are right to call it out.

Mr. JOYCE. Mr. Johnson, in the few seconds that I have left, are you aware of a model of public-private partnership that can lay the groundwork in the future of our Nation's cybersecurity?

Mr. JOHNSON. Yes, sir. I mentioned this in my opening. CSRIC, back in 2015, recommended to the FCC a model of partnership between the FCC and DHS to engage network operators in particular in a—in a trusted, confidential partnership environment for security. In some ways, it was prescient because this is what they ended up doing during the COVID pandemic. But I think formalizing that, basically picking up those CSRIC recommendations and seeing how they apply to the present, is an important model.

Mr. DOYLE. The gentleman's time has expired.

Mr. JOYCE. Thank you, Chair.

Mr. DOYLE. The Chair sees Mr. Cárdenas is joining us remotely.

Tony, you are recognized for 5 minutes.

Mr. CÁRDENAS. Thank you, Coach—I mean Chairman. And by the way, I am working on Senator Padilla to join us on the field.

Thank you, Mr. Chairman and Ranking Member, for having this very important issue, which is, unfortunately, going over most American's heads, but it is in their hands every single day and it is in their lives. And I hope that we can pass this critical legislation that my good colleagues on both sides of the aisle have introduced [inaudible].

I want to take a point of personal—one of the witnesses mentioned that he is an engineer. I am proud to be an engineer myself. But kind of made it very clear—politician reminded me of my mother. When I went off to college, she gave me a hug and said she was very proud of me. When I told her I was going to run for office, she gave me a hug and said she would pray for me. When I got my degree, she hugged me again and said she was very proud of me. When I got elected, she hugged me again and said she will pray for me. So you brought back some memories from a long time ago.

So on a serious note, I think it is important that we all understand how important the supply chain security is. Wireless security and innovation are very technical, and I wanted to talk about these important issues here so we can get it on the record. As part of this legislative process, I think it is critical that we have these very important issues and that we hopefully get our public, our constituents to understand how important they are.

First, it is vital to understand and identify any problems in our current systems under our increasingly digital lives. That is why bills like Rep. Eshoo and Kinzinger's Understanding Cybersecurity of Mobile Networks Act is so critical. It gives us insight into the vulnerabilities of our networks so providers can address them.

Our communications networks are built from materials and components from all over the world. It is also important to identify where these come from and that all of these components are se-

cure. That is where the Information and Communications Technology Strategy Act comes in.

Second, it is important to prepare for the future, which is why we need legislation like the FUTURE Networks Act, to make sure that, while the U.S. continues to be the leader in technological innovation, we get ahead of any security issues and ensure we are doing what we can to help all Americans use new technologies to make our lives better.

The third piece of the puzzle that we need to talk more about and what I want to focus on today is the safety of the American people. While on a national level we need to make sure our networks and supply chain are protected, it is in the homes and the small businesses and businesses across America that people are subject to hackers, and they can do tremendous damage. We need to work together to do our part. That includes companies, government, and every single one of us.

One way to play our part as citizens is by being empowered with simple, high-impact methods we can use to increase cybersecurity of our devices and networks. That is why I am proud to support the American Cybersecurity Literacy Act.

I have a question for you, Mr. Srihari. We know that technology is critical to everyday life. It is how we stay connected with loved ones, work, get an education, among other things. It is how we get to see my grandchildren in Los Angeles when I am in Washington, DC.

While this technology can expand our quality of life infinitely, we also know it is growing more and more complex. We need to make sure our communities have the tools to use tech safely.

Can you talk about some of the common threats consumers are facing today?

Mr. SRIHARI. Sure. I mean, when we are talking about cybersecurity, we are talking about malware being installed, we are talking about phishing attacks, social engineering exploits. If you look at the statistics on this, although the numbers vary, everyone agrees that at least a majority and some say even 80, 90 percent of cyber attacks are because of things as common as basic password problems or basic user error. These are not complicated, technical exploits here. And the effects can be very harmful, either to businesses or personally, causing billions and billions of dollars in economic damages every year.

So I think at a very basic level, educating the public at large on these issues would have a huge beneficial effect for the economy overall, but also make a real difference in people's lives to prevent these kinds of problems from happening.

Mr. CÁRDENAS. So literacy is something that we can all practice on a daily basis: individuals, small businesses, large businesses, et cetera.

Mr. SRIHARI. Absolutely. And that is where it starts. And a lot of the problems that we see in very large organizations are because one individual made a mistake somewhere deep down the line and it trickled all the way up and caused a major outage. So, yes, I think you are right.

Mr. DOYLE. The gentleman's time has expired.

Mr. CÁRDENAS. Thank you very much. My time has expired.

I yield back. Thank you, Mr. Chairman.

Mr. DOYLE. The Chair sees that Mrs. Fletcher has joined us, So we are going to recognize her for 5 minutes. She is joining us remotely.

Mrs. FLETCHER. Well, thank you so much, Chairman Doyle. And thanks to you and Ranking Member Latta for holding this important hearing today and to all of our witnesses for taking the time to testify.

American businesses, consumers, and innovators, and the economy will benefit if the United States maintains our leadership on 5G, 6G, and future generations of wireless networks and devices. Security of these systems is of paramount importance. We have been discussing that all morning, the cyber attacks that we have seen across a variety of sectors just this year. And in response to what my colleague Mr. O'Halleran said, you know, issues that we have been talking about for a long time, and it is important now for Congress to pass sound policy that will protect users and networks as the world continues to become more interconnected.

So, Mr. Brenner, how will the bills that we are considering today, like the FUTURE Networks Act, help us maintain our leadership on wireless connectivity?

Mr. DOYLE. Mr. Brenner, turn your microphone on.

Mr. BRENNER. Thanks so much for the question. I am going to repeat what I said previously, because there are two key things that that bill can do.

One, it will start the multiyear process of working with the FCC and other parts of the Government to identify the spectrum that 6G will ultimately need to be rolled out in. And it is completely a great idea to start on that as early as possible.

And then the second thing it can do is create a forum to work on the siting issues, because we are going to need lots of sites to put the towers on in order to ensure a universal connectivity with the next generation of wireless.

Mrs. FLETCHER. Well, thank you for that. And that is an issue that we have been focused on in my district in Houston, where, of course, we have a large effort underway across the city to have 5G connectivity and, of course, a lot of the infrastructure pieces in place, and so this has been a real focus in our community. And I think it is important that, you know, we help share some of those—some of those lessons that we have learned about how we can facilitate that.

I want to turn to another question or two with the time I have left, but really thinking about these threats that we have been talking about today.

Mr. Johnson, as you noted in your testimony, you know, COVID really put a spotlight on the critical role that our communications networks play in our lives. We are seeing it right now as we continue to be connected here in Congress and as people across the country are connected digitally following this difficult year. But we also know how important it is that we stay vigilant to protect these networks from cyber attacks and these unwanted intrusions by adversaries.

So we talked about this a little bit, but I would love just a sort of a summary of how the Government can stay on top of these

threats and vulnerabilities while at the same time ensuring that manufacturers and others can innovate, as several people have mentioned today. But, you know, maybe if you could address that, Mr. Johnson, and then if there is any time left, Mr. Boswell or Brenner, if you wanted to add anything from the industry perspective, that would be helpful.

Mr. JOHNSON. Great. Thank you, Congresswoman. I will try to leave some time for my colleagues here.

I think the best way for the Government to stay on top of these threats is to work in partnership with the companies that are addressing these threats every day. The network operators, trusted suppliers, other parts of the ecosystem, this is their core business. This is what they do. And they have, frankly—and, you know, the U.S. intelligence services may know some foreign adversary intentions in different ways than the companies do, but, frankly, the collective expertise and resources of the ICT industry has a much better finger on the pulse than any other institution. So we need to leverage that expertise through partnerships that they can trust.

Mr. BOSWELL. Thank you, Mr. Johnson.

Yes. If I could follow on with that, it is why I get up in the morning, right. That is why my whole team goes to work every day is to ensure the security of Ericsson Solutions but also the networks of our customers, and ultimately that means that it is U.S. critical infrastructure.

And in some of the different groups that you have heard mentioned today, whether it is CSRIC or the NSTAC or even some of the work that DHS has done across different supply chain task force, there are three key things that kind of come up as patterns. First is that we must secure the communications itself end to end. Secondly, we must ensure the resilience of the network. And third, we must protect the integrity of the supply chain.

Those patterns come up again and again, and we worked hand-in-hand with different government agencies really to put those into best practice policies that others can follow with.

Mr. DOYLE. The gentlewoman's time has expired.

Mrs. FLETCHER. Well, thank you so much, Mr. Boswell. My time has expired.

Thank you, Mr. Chairman.

Mr. DOYLE. OK. I see we have no more Members for questions, so we are going to close this hearing.

We want to thank the witnesses for their participation in today's hearing.

I see we have nothing to insert into the record. So I would remind Members that, pursuant to committee rules, they have 10 business days to submit additional questions for the record to be answered by the witnesses who have appeared. I would ask each witness to respond promptly to any such questions that you may receive. So we want to thank all our witnesses for attending today.

And, with that, the committee is adjourned.

[Whereupon, at 1:22 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Health Chairwoman Anna G. Eshoo

Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains"

June 30, 2021

Thank you for holding this important hearing, Chairman Doyle and Ranking Member Latta.

Securing our wireless networks is a matter of national security because compromised equipment can lead to surveillance of our communications by our adversaries, including foreign governments. This is why I've made the issue a top priority for over a decade. I first wrote to the FCC on November 2, 2010, about the national security risks created by Huawei and ZTE, and I've remained focused on this issue since then.

I'm pleased to see the many important bills that we'll discuss today, including three bipartisan bills I've led:

- H.R. 2685, the *Understanding Cybersecurity of Mobile Networks Act*, is legislation I authored with Rep. Kinzinger that requires the NTIA to conduct an in-depth study of the cybersecurity of the 2G, 3G, and 4G networks in our country. While there have been many disparate efforts to examine vulnerabilities, we lack a comprehensive understanding of the issue. While 5G and 6G are critical for our telecommunications future, most of our calls, texts, and data still traverse through legacy networks which present threats to the whole network.

- H.R. 3919, the *Secure Equipment Act*, is legislation I partnered with Rep. Scalise to introduce. The bill prohibits the FCC from issuing new equipment licenses to companies on the FCC's list of entities that pose a national security threat. Senators Rubio and Markey have companion legislation in the Senate, and Acting Chairwoman Rosenworcel and Commissioner Carr – a Democrat and Republican respectively – support the bill.

- H.R. 4055, the *American Cybersecurity Literacy Act*, is a bill I introduced with Rep. Kinzinger to require NTIA to develop and conduct a cybersecurity literacy campaign to educate Americans about cyber vulnerabilities and best practices to reduce associated risks. Government is only responsible for approximately 20 percent of cybersecurity and individuals and companies are responsible for 80 percent. Americans can vastly reduce harm experienced by cyberattacks by heeding best practices, and the federal government can help spread knowledge about what people can do to reduce their risk.

I'm also pleased that we'll be discussing the advancement of Open RAN and directing agencies to begin to think about 6G.

I look forward to a productive hearing and I yield back.

Attachment—Additional Questions for the Record

Subcommittee on Communications and Technology
Hearing on
"A Safe Wireless Future: Securing our Networks and Supply Chains"
June 30, 2021

Mr. Jason S. Boswell, Head of Security Network Product Solutions, Ericsson North America

The Honorable Cathy McMorris Rodgers (R-WA)

1. This Committee has a history of bipartisanship when it comes to enhancing network security. We worked together to pass the Secure and Trusted Communications Networks Act to get Huawei out of our networks, and just last year worked to pass the USA Telecommunications Act to promote the deployment of OpenRAN compatible technology.

   While OpenRAN shows promise to increase vendor diversity, we also recognize that this is a new concept. Mr. Boswell, at the hearing we discussed H.R. 4032, the OpenRAN Outreach Act, which would establish a government office to provide technical assistance to smaller companies interested in deploying OpenRAN compatible technologies.

   a. What role do you think the government should play in the development and deployment of OpenRAN compatible technology?

RESPONSE: Congresswoman, you are correct, Open RAN does show promise. You are also correct that it is a new concept. There is still much work to be done before these potential promises are realized. In its nascent stage, work is still incomplete in many areas, and challenges remain, including with regard to network security.

In determining what role, if any, the government should play in the development and deployment of Open RAN compatible technology, Ericsson believes that the guiding principle should be technical neutrality. The government should not pick winners and losers. Carriers should decide what technology is best for them based on the unique needs of their individual network architectures. History has demonstrated the best way to maximize the benefits of new technologies is to promote a competitive marketplace and let market forces work. It is important that the U.S. government support a technology neutral environment that promotes innovation, allowing the private sector to lead and the market to determine the "winners." The best price/performance ratio should carry the day. History attests to the wisdom of market-led technological advance. U.S. leadership in technology in 4G and 5G has been achieved via technologically neutral policies, without any government mandates that tipped the scales.

As I said in my written testimony, regarding policy to facilitate Open RAN's development and deployment, Ericsson itself sees no barrier to deploying Open RAN solutions. Ericsson's Cloud RAN is a major step on the journey to a secure Open RAN solution that meets the needs of U.S. critical infrastructure. It allows operators to run Ericsson RAN software using commercial off the shelf hardware and the third-party cloud stack (e.g., platforms provided by IBM/Red Hat, Linux, HPE, Intel, and many others). We can find nothing that would impede Ericsson or any other vendor from competing in the marketplace for Open RAN products and services today.

There are, however, steps the government is appropriately taking to encourage the development of more open network architectures generally. The government should encourage increased transparency and security of Open RAN deployments. We commend the FCC's recent announcement that it will create two additional innovation zones in collaboration with the National Science Foundation.

Additionally, it is appropriate for the government to encourage U.S. industry participation in standards development organizations (e.g., 3GPP, Institute of Electrical and Electronics Engineers, Internet Engineering Task Force) to assure industry-led forums remain the principal organizations for standards development. I note that H.R. 3003, the "Promoting United States Wireless Leadership Act of 2021," which recently was passed by the full House of Representatives is designed to encourage such participation.

2. Last October, Sweden enacted a 5G equipment sales ban against Chinese companies Huawei and ZTE, following suit with actions taken by the United States to secure our networks from foreign bad actors.

   Just last month, the Stockholm Administrative Court upheld this action. Over the past several months, it has been reported that your CEO has lobbied against this ban in Sweden, which runs counter to the actions taken by the United States to push allied countries to remove this equipment from their networks.

   Given the topic of our hearing, I am concerned that Ericsson, one of the top trusted vendors in the United States, appears to be taking a different position on Huawei than the U.S. government.

   a. How does Ericsson engage with Huawei when discussing cybersecurity or developing standards for equipment? Do you agree that Huawei equipment poses a national security threat when in networks?

RESPONSE: We do not engage with Huawei on cybersecurity issues. With respect to Ericsson's work in standards bodies, like all companies involved with global standards, we work with dozens or even hundreds of companies across different standards organizations. Whether any specific equipment poses a national security threat in networks is a decision for government intelligence experts, not private companies. I will say that when governments have conducted security assessments, Ericsson has been designated as a trusted and secure supplier.

The Honorable Bob Latta (R-OH)

1. H.R. 4028, introduced by Representative Long, directs NTIA to identify critical components of our communications networks that we may be overly dependent on and come up with a whole of government strategy to help diversify and improve the economic competitiveness of trusted vendors. What steps are Ericsson taking already to diversify, and do you have any recommendations for how the Federal government can be a better partner?

RESPONSE: We agree that the having a healthy competitive ecosystem of trusted vendors is critical. We believe that trusted vendors, like Ericsson are competitive, both in the U.S. and globally. In fact, I'm proud to say that Ericsson is now the leading global vendor of 5G Radio Access Network (RAN) equipment. And we face stiff competition from other trusted vendors. With regard to diversification, Ericsson has taken steps to diversify its supply chain by moving manufacturing closer to our customers. Here in the U.S., this strategy led us to open a $100 million 5G smart factory in Texas last year, the first large scale 5G factory in the U.S. We are manufacturing Advanced Antenna System radios at the factory to enable 5G deployments in the U.S. This factory is just one example of Ericsson's commitment to the U.S. as I discussed in my testimony. We have successfully managed the 40-year evolution of wireless technology from 2G to 5G of mobile in the U.S. and the U.S. has enjoyed the economic benefits as a result of this leadership. We hope that the government will continue to recognize this significant and continuing contribution. We encourage the government to maintain technical neutrality when considering telecommunications policies and to continue to include trusted vendors, like Ericsson, when considering programs to support U.S. leadership in 5G and beyond.

The Honorable Bill Johnson (R-OH)

1. The U.S. is actively deploying 5G, which has more secure architecture than legacy services in 2G, 3G, and even 4G. I understand that Ericsson recently reported approximately 580 million 5G subscriptions will be active by the end of 2021 —while North America is second among regions adopting 5G, most of those 2021 adoptees are in Northeast Asia, including China. How can the United States encourage faster deployment of secure 5G services?

    a. While it was not part of our hearing, you may have seen that I've sponsored H.R. 1056, the Wireless Broadband Competition and Efficient Deployment Act, which exempts collocations of wireless facilities from the requirement to prepare an environmental or historic preservation review. Would legislation like this help to speed up the upgrading of existing infrastructure to deploy 5G?

RESPONSE: Yes. Legislation like H.R. 1056 would help accelerate the upgrading of existing infrastructure to deploy 5G. The historic and/or environmental review process can add an additional 90 days to the application process. In many states the process to review simple antenna installations on existing infrastructure is nearly the same as if a developer was building a new apartment complex. We agree that if an installation involves erecting a new tower or placing

ground equipment outside an already-analyzed parcel, a review is appropriate. But forcing operators to go through the environmental process on an already-analyzed parcel is redundant and adds unnecessary time to the deployment process. As for historic areas, we agree that new installations on buildings in a designated historic zone need to match the style of the building, and the industry works hard to make sure the installation on a historic building is not obtrusive.