S. Hrg. 116–582

5G SUPPLY CHAIN SECURITY: THREATS AND SOLUTIONS

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

MARCH 4, 2020

Printed for the use of the Committee on Commerce, Science, and Transportation

Available online: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
52–663 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

John Keast, *Staff Director*
Crystal Tully, *Deputy Staff Director*
Steven Wall, *General Counsel*
Kim Lipsky, *Democratic Staff Director*
Chris Day, *Democratic Deputy Staff Director*
Renae Black, *Senior Counsel*

CONTENTS

WITNESSES

APPENDIX

5G SUPPLY CHAIN SECURITY: THREATS AND SOLUTIONS

WEDNESDAY, MARCH 4, 2020

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m. in room SR–253, Russell Senate Office Building, Hon. Roger Wicker, Chairman of the Committee, presiding.

Present: Senators Wicker [presiding], Thune, Blunt, Fischer, Sullivan, Gardner, Lee, Johnson, Young, Scott, Cantwell, Peters and Rosen.

OPENING STATEMENT OF HON. ROGER WICKER, U.S. SENATOR FROM MISSISSIPPI

The CHAIRMAN. Good morning and welcome to the newly restored Committee room of the Commerce Committee.

I want to thank Senator Blunt of the Rules Committee and the Architect of the Capitol for their effort in restoring this room and welcome all of you to a history-making hearing, the first hearing in the newly opened room.

Today, the Committee convenes to discuss the security and integrity of the telecommunications supply chain. That is to say, the equipment and services that make up a communications network.

I welcome our distinguished panel of witnesses and thank them for appearing. Today, we'll hear from Mr. Steven Berry, President and Chief Executive Officer of the Competitive Carriers Association; Mr. Jason Boswell, Head of Security, Network Product Solutions at Ericsson; Ms. Asha Keddy, Corporate Vice President and General Manager of Next Generation and Standards at Intel; Mr. Mike Murphy, Chief Technology Officer, Americas at Nokia; and Dr. James Lewis, Senior Vice President and Director of the Technology Policy Program at the Center for Strategic and International Studies.

Closing the digital divide and positioning the United States to win the global race to 5G are priorities for this committee. Over the past several months, we have been discussing the wide-ranging economic and social benefits that broadband connectivity has delivered to communities across the country.

We've also discussed the promise of 5G networks to build upon these past advances and create new opportunities.

Our continued ability to connect all Americans and provide access to next generation technology will depend in large part on the security of the Nation's communications infrastructure.

Over the past few years, the U.S. Government's intelligence officials and international allies have determined that telecommunications equipment from certain vendors, such as Huawei and ZTE, poses a national security risk.

Foreign adversaries and enemies of the United States have the capability of using this compromised equipment to spy on Americans, steal our intellectual property, and otherwise disrupt our way of life and economic well-being.

Today, both Congress and the Trump Administration have taken a number of actions to address these security threats and protect our networks and devices from hostile exploitation. These actions include banning the use of Huawei and ZTE components in government systems, prohibiting the use of the Universal Service Funds to purchase communications equipment and services from Huawei and ZTE, and other high-risk suppliers, and adding Huawei and its affiliates to the entity list.

Most recently, Congress passed the Secure and Trusted Communications Networks Act. When signed into law by President Trump in just a few days, this law will establish a critical Rip and Replace program for small and rural telecommunications operators to remove compromised equipment from their networks and replace it with components from trusted suppliers.

While this is a meaningful step forward in safeguarding the security of the Nation's communications systems, the unfortunate reality is that our networks have already been compromised by foreign adversaries.

We are seeing more reports that Huawei can covertly access mobile phone networks around the world. At the same time, some of our close allies are granting Huawei access to their communications systems. These are troubling developments.

We need to do more to shore up our own network defenses against hackers and state-sponsored actors, especially in our Nation's rural and underserved communities. This effort will require the development of a comprehensive strategy to secure the telecommunications supply chain.

Currently, Huawei maintains the largest global market share of telecommunications equipment. The absence of a viable and affordable American or European alternative for end-to-end telecommunications components, including radios, chips, software, and devices, has enabled Huawei to increase its global influence.

At a time of rising global demand for 5G equipment, I hope witnesses will discuss what more Congress and the Administration can do to support trusted suppliers, invest in new technologies, and expand the domestic market for 5G network components.

There are a number of international standard-setting organizations, such as the Third Generation Partnership Project or 3GPP and the International Telecommunications Union that are developing technical standards for 5G. U.S. participation in these organizations is also key to a secure telecommunications supply chain.

Today's hearing is an opportunity for witnesses to discuss how to increase U.S. engagement in the standards development process. This will help ensure American technical expertise and priorities are considered in the development of next generation technologies.

Finally, I hope we will learn about how the telecommunications industry can improve its cyber hygiene, meaning what best practices companies could adopt to mitigate risks to vulnerable supply chains.

I also hope we will learn about what more the FCC can do to secure legacy networks and manage security risks in the transition to 5G.

Let me again welcome our witnesses and thank them for joining us, and I recognize my friend and Ranking Member Senator Cantwell.

STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Thank you, Mr. Chairman, and thank you for holding this important hearing.

I, too, want to thank Senator Blunt for his work in getting us back into our normal hearing room.

Today's hearing, obviously, we have a lot of great witnesses here, and thank you for traveling to be here.

We've heard a lot about 5G networks and how it's going to revolutionize everything from sectors of our economy to advancements, but none of this will happen unless we make the system secure.

Yesterday, we had a hearing as part of our review of the budget for energy and we were focusing on our Nation's grid and the fact that just recently, an attack on our grid in the West was the first time an actor had actually brought down a power system for more than 12 hours.

So it's no longer just people searching around and looking at our power plants. Now, actors are starting to bring what are essential services to a halt, and these are important issues for us to address throughout our system.

So far, the discussion by policymakers about how to keep unsecure networks and equipment out of our domestic networks has been the focal point, but obviously eliminating the threat posed by this equipment is the highest priority. We can't just simply look at that issue. We need to make sure that we are a loud voice across the globe for no government backdoors to any security network.

By mitigating this, we are helping to communicate what needs to be done. I believe it's an imperative that the U.S. and its allies foster a truly secure, diverse, and reliable supply chain for communications equipment. We need to assure the communications systems are secure and that the connections to those systems and software are also secure.

To accomplish this, first and foremost, we need a broader strategic plan, and I know that recently our bill that we passed out by our colleague, Senator Cornyn, in July was about getting the President to send to Congress a much-needed strategy on 5G, and hopefully we'll see more details on that soon.

But we must also build a forceful global coalition of countries to share our values and respect property rights and the Rule of Law, and we need a smart multinational approach to this. And so I hope that, Mr. Chairman, we'll continue to work with our colleagues on the Intel Committee and on the Foreign Affairs Committee to make sure that this is also being accomplished.

We must create incentives for other countries to use communication equipment that does not contain a government backdoor access, and the United States should have a great source of allies to work with us on these issues.

So again, appreciate this hearing this morning. I think it's important to continue to clarify U.S. leadership on this issue and how we move ahead, and I appreciate the fact that we have so many great witnesses to talk about what these immediate next steps are in the legislation that has gone to the President's desk.

Thank you, Mr. Chairman.

The CHAIRMAN. And thank you, Senator Cantwell.

We have a vote on the Senate Floor scheduled for around 10:30 and so we'll just do the best we can sharing the gavel and getting back and forth, but we are delighted to have the testimony.

Your written statements will be included in the record in full and we recognize each of you for around five minutes to summarize your testimony.

Mr. Berry.

STATEMENT OF STEVEN K. BERRY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, COMPETITIVE CARRIERS ASSOCIATION

Mr. BERRY. Thank you, Mr. Chairman.

[Off microphone comments] for every American in Rural America, reliable broadband maps. I look forward to your successful completion of the Broadband Data Act and it's signed into law. So from everyone from rural America, big thank you to this committee.

Chairman Wicker, Ranking Member Cantwell, and members of the Committee, thank you for the opportunity to testify about security and integrity of the telecommunications supply chain, both for existing wireless networks and for the Nation's future 5G.

CCA is the Nation's leading association for competitive wireless carriers as well as the vendors and suppliers serving that ecosystem. CCA and its members fully support efforts to protect networks from cyber and national security threats.

I strongly commend this Committee's bipartisan efforts to send the Secure and Trusted Communications Networks Act to the President. This important legislation addresses many key concerns. It provides all carriers with clear direction and, importantly, creates a fund to help small carriers replace covered equipment.

Since I last appeared at this Committee, there has been a lot of talk about what steps small carriers must take to secure their networks and your actions, as a matter of fact your legislation, will allow these carriers and government officials to not just talk the talk but actually walk the walk.

Wireless networks are providing connectivity for innovations ranging from health, education, and public safety to economic and social transformations. All carriers are focused on providing secure connectivity against the ever-growing array of threats. The transition to 5G networks provides an opportunity for all carriers to build in security as a basic function.

The challenge is heightened by carriers that have equipment in their networks from companies deemed by Federal agencies to pose a national security threat.

Now let me be clear. Most CCA members do not have covered equipment in their networks. For those that do, often they provide service to their own rural communities, operating where other carrier providers don't provide service on the thinnest of margins to connect their neighbors. These companies are owned by and employ Americans in their local communities and I can assure you these patriots want to take whatever steps necessary to ensure our national security. Through your actions, these carriers will have a program to support replacing covered network elements.

Chairman Wicker, I completely agree with your floor remarks when you said some things are worth paying and protecting America is worth paying for.

The undertaking to replace existing equipment is unprecedented, historic, never been done. Networks in operation today were built over years, actually decades, and such a significant undertaking will be all-encompassing.

Further, this task must be completed in a way that keeps rural Americans connected. For all the talk about Rip and Replace, carriers must actually create and execute individual plans that replace and then rip. They must maintain service before decommissioning. Anything less threatens the loss of connectivity in rural America, including access to 9–1–1 and public safety services.

These carriers are essentially attempting to rebuild the airplane in midflight, and the challenge of securing networks does not end here. As we enter the 5G era, there are new opportunities for all carriers to build security into the networks from the ground up.

There are three main factors for industry and policymakers going forward. Number 1, all carriers must have clear guidance and information from the Federal Government regarding security. You did this. Your legislation facilitates information sharing specifically for small providers.

Number 2, secure trusted network equipment must be available for all carriers. The Act directs the creation of a list of suggested replacements that would allow carriers with and without covered equipment to confidently make the decisions that they will need. Flexibility will be the secret sauce to this success.

And Number 3, new technologies hold the promise to enhance security, spur innovation, and save costs. We should explore virtual technologies. However, policymakers should not mandate technologies. If new technologies deliver on ther promise, they will compete successfully in the marketplace.

And in closing, thank you again for the exceptional leadership in passing the Secure and Trusted Communication Networks Act. CCA is committed to working with not only all the shareholders, the stockholders, and stakeholders, as you would say, to accomplish the challenging task of securing our networks while we maintain communications services for millions of consumers in rural America, and so thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Berry follows:]

PREPARED STATEMENT OF STEVEN K. BERRY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, COMPETITIVE CARRIERS ASSOCIATION

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to testify about the security and integrity of the telecommunications supply chain, both for existing wireless networks and for our Nation's 5G future.

I am testifying on behalf of Competitive Carriers Association ("CCA"), the Nation's leading association for competitive wireless providers. CCA is composed of nearly 100 carrier members ranging from small, rural providers serving fewer than 5,000 customers to regional and nationwide providers serving millions of customers, as well as vendors and suppliers that provide products and services throughout the mobile communications ecosystem.

CCA and its members fully support efforts to protect and harden networks from cybersecurity and other national security threats. Press reports and actions by the Federal Government continue to underscore the threats posed by certain companies and foreign adversaries. To address these threats, I particularly commend this Committee's bipartisan leadership in sending the Secure and Trusted Communications Networks Act to the President for enactment. This important legislation addresses several key concerns of competitive carriers that are working to secure their networks. In particular, the legislation provides certainty regarding what actions small carriers must take to modify their existing networks and establishes a fund to ensure that resources are available.

Beyond the immediate attention on network security, we must also not lose focus on the economic security threats we face as a nation as we compete globally to provide the latest innovations, powered by wireless communications. Establishing American leadership for 5G network deployments, including the potential for a greater role in the 5G supply chain, is an important goal, and one that can only be achieved by ensuring that all Americans have access to the latest services, both in urban population centers as well as rural America. In fact, rural areas stand to enjoy the most immediate and significant benefits through expanded access to the latest wireless services. No one will win the so-called "race to 5G" without connecting the millions of people living in rural America.

While wireless networks are providing connectivity for innovations ranging from health and public safety advances to economic and social transformations, these connections must be secure. All carriers are therefore focused on ensuring that they are providing secure connectivity amidst an ever-growing array of potential threats. The transition to 5G networks provides an opportunity for all carriers to build in security as a basic function of network architecture and management.

Security threats are particularly acute for carriers that have equipment or services in their networks from companies deemed by Federal agencies, including the Federal Communications Commission ("FCC"), to pose a "national security threat to the integrity of communications networks or the communications supply chain." To be clear, most CCA members do not have covered equipment in their networks. Those that do often provide service to their own rural communities, operating where no other carrier will provide service and at the thinnest of margins to connect their neighbors. These companies are owned by and employ Americans in their local communities, and I can assure you that these patriots want to take whatever steps are necessary to ensure our national security.

Whether or not a carrier has covered equipment in its immediate network, removing insecure network elements is a priority shared across the industry. Telecommunications networks provide value to all consumers through the network effects of connectivity, and networks must interconnect with each other. Further, through roaming and other arrangements between carriers, as you travel the country you have likely enjoyed service from rural carriers, whether you realize it or not. Accordingly, all networks must be secure.

This hearing is timely, with actions being taken not only by Congress, but also by the FCC and an Executive Order from the President. While the challenge is significant, and the legislative and regulatory policy directions are unprecedented, I have confidence that appropriate policies from the Federal Government will provide all carriers with the guidance and certainty they need to secure telecommunications networks. Through cooperative efforts and flexible policies, and funds for replacement, the removal of covered networks elements, where necessary, can be achieved. Such action will support new technologies and innovations while allowing market forces to advance secure services and make the latest wireless technology available for all carriers, whether they serve customer bases that are rural, regional, or nationwide.

All Carriers Must have Clear Guidance from the Federal Government Regarding Security

As a foundational step, all carriers must have the information and guidance from the Federal Government to confidently make decisions to secure their networks. With respect to the need for clarity, I appreciate the clear message sent by Congress through the Secure and Trusted Communications Networks Act regarding what network equipment is deemed to be insecure and must be removed from existing networks. This clarity is particularly important for smaller carriers that may not have dedicated staff focused exclusively on security issues or may not have the necessary clearances to engage directly with the intelligence community regarding potential threats.

I strongly encourage the Federal Government to continue to provide clear, unambiguous directions regarding the national security needs for communications networks so that government and industry can define a clear pathway for enhanced security and allocate resources to sustain these priorities. Such efforts help improve the security hygiene across the entire telecommunications industry, for small carriers and nationwide providers alike. Provisions in the Secure and Trusted Communications Networks Act that facilitate information sharing, specifically for smaller providers, will help advance this goal.

CCA has taken several steps to ensure that our members have access to the information they need to make confident decisions regarding potentially sensitive issues. For example, nearly a year ago approximately three dozen CCA members, including members with and without covered equipment, participated in a bipartisan, classified briefing on wireless security issues with the U.S. Senate Select Committee on Intelligence. I would like to thank Senators Warner and Rubio for hosting CCA members and key leaders from the Intelligence community to ensure that all carriers are provided with the information they need to make decisions to provide secure telecommunications services to their customers.

I am also very pleased that we were able to continue our educational effort by partnering last year with the U.S. Chamber of Commerce to conduct three Rural Engagement Initiative sessions. At these events we brought together numerous stakeholders, including representatives from Tier II and Tier III carriers serving rural areas, security experts from leading American and international vendors and suppliers, and key senior government officials from the Department of Homeland Security, Department of Justice, Federal Communications Commission, and Department of Commerce together in three different locations—Denver, CO, Jackson, MS, and Chicago, IL—to have frank discussions regarding current threats, potential solutions, and the roadmap for network operations in the years ahead. These conversations allowed both government and industry to gain a better sense of the strategic threats, and a clearer understanding that there is no one-size-fits-all solution to mitigating these threats. I truly appreciate our partnership with the U.S. Chamber of Commerce on this effort to bring critical information to all carriers. I also would like to particularly thank the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") for taking a lead role on behalf of the United States Government in these sessions, which brought tremendous value to competitive carriers and facilitated the direct flow of information between government and industry stakeholders. Building upon these conversations, I look forward to welcoming CISA as a keynote speaker at CCA's upcoming Mobile Carriers Show later this month.

Congress has Provided Clear Authority and Established a Fund to Secure Existing Networks

The Secure and Trusted Communications Networks Act not only provides clarity regarding what elements must be removed from existing networks, it importantly creates a fund to facilitate replacement for smaller carriers serving rural areas. I completely agree with your remarks, Chairman Wicker, on the Senate floor late last year that "some things are worth paying for, and protecting America, protecting our electronic system, our broadband communications. . .is worth paying for."

I am encouraged that this sentiment shares bipartisan support not only in Congress but also at the FCC. As FCC Commissioner Geoffrey Starks noted last fall at CCA's Annual Convention, "This is a national problem that deserves a national solution, and we shouldn't expect small carriers—who acted legally and in good faith—to replace their insecure equipment on their own." Recent Congressional action will provide needed resources for the replacement of covered equipment, an important step that is particularly needed for carriers who are unable to cover the costs of replacement without financial assistance from the Federal Government.

As the new fund is established and administered by the FCC, I am hopeful that resources will be available so that carriers can move expeditiously to replace covered network elements. This means that after a carrier with covered equipment has established a clear plan for replacement and removal of networks elements, they will have access to funding both as the process begins as well as at specified benchmarks throughout the process. Such access to needed resources recognizes that networks that were not initially economical to construct absent support mechanisms are unlikely to be able to finance the project management process without resources available long before certification that covered elements have been completely removed. Additionally, as the removal process moves forward, policymakers should allow for carriers to triage their networks and focus on the most significant vulnerabilities first. Specifically, policymakers should consider prioritizing replacement of core network and routing elements first, and radio and edge network elements thereafter, in recognition of using available resources to prioritize the highest potential threats.

While the legislation that recently passed establishes a swift one-year timeframe, I appreciate the inclusion of a waiver process to ensure that carriers that are unable to complete changes to their networks in such a rapid fashion remain eligible for support. Several factors, including available spectrum resources, equipment availability, limited windows to build in certain harsh geographic areas, permitting processes, the need for testing and configuration of new equipment, and even the availability of a properly trained workforce will all impact the time necessary for each impacted carrier to complete the transition process.

Going forward, I would be remiss not to mention concerns from our carrier members that reverse auction procedures used to distribute support for providing service in rural areas can lead to a race-to-the-bottom where low costs are prioritized above all else. Several carriers that have covered equipment in their networks today made vendor selections a decade ago in order to meet the reverse auction structure of Mobility Fund Phase I, where winning auction bids were those that had the lowest cost to serve the greatest number of road-miles. Despite there being no prohibited vendor selections at the time, it is now clear that this mechanism led to undesirable consequences for several carriers. While the FCC now has rules in place prohibiting using USF support for specific vendors going forward, security priorities should be appropriately funded so that other unintended consequences of funding least-cost networks can be avoided in the future. All funding recipients must be good stewards of taxpayer funds, but we should not simply fund the cheapest possible networks at the expense of all other priorities. There should be some mechanism in the funding process that recognizes and rewards resiliency and security enhancements, prioritizing providing reliable and secure connectivity for consumers.

Replacing Covered Network Elements Must Precede Decommissioning to Maintain Connectivity

With clear guidance regarding network elements that pose security threats and a newly established fund available to replace them, carriers are eager to begin the work to transition their networks and continue to move forward to best serve their customers. To ensure that Americans in rural areas do not lose connectivity during this process, including to voice connectivity and 9–1–1 emergency services, important safeguards must be in place.

While those inside the beltway often refer to the process as “rip and replace,” in practice carriers will typically need to “replace, then rip” to ensure that the consumers served by rural carriers do not lose service. This is a significant challenge for carriers, as a separate, standalone network must be established and stood up alongside current services before carriers can transition traffic to the new equipment and then decommission the covered elements. Networks in operation today have been built over years or even decades, and such a significant rebuilding will be all encompassing, including not only funding but also technical and logistical resources. Further, each carrier’s network is unique, and accordingly there is not one plan or solution that can be followed by all carriers in this situation. Individual carriers’ plans may be particularly challenging based on any given carriers’ spectrum portfolio, which will need to support both new and legacy networks during the transition process, as well as the carrier’s access to backhaul and other network characteristics. Again, only a few CCA carrier members have covered equipment in their networks, but all carriers understand the collective impact on their colleagues, and recognize that successfully addressing this challenge now will help everyone as we move to 5G.

Additionally, some covered equipment is outdated technology that is no longer manufactured or supported for new construction by any vendor. Equipment manufacturers generally are no longer making 2G and 3G equipment, and it would make little sense for any carrier to deploy a 2G or 3G network today. Accordingly, while the Secure and Trusted Communications Networks Fund should not create a windfall, resources should be available for carriers to provide like-for-like services that leave carriers more prepared at the end of the transition process to utilize other resources to upgrade networks to the latest generation of services in the future. For example, if a network with covered elements supports 2G and 3G CDMA voice products, the replacement should also support voice services, even if this means an enhancement in the network to support VoLTE voice services that could subsequently be upgraded as the carrier deploys 5G. This approach will ensure that the transition process does not leave a rural area stranded on legacy technologies while the rest of the industry advances. That is not a windfall but a reality reflecting the state of today's technology.

New Technologies can Help Secure Networks; Mandates should not Stifle Innovation

Removing covered network elements, as supported by the Secure and Trusted Communications Networks Act, is a critical step to secure today's networks, and several concepts included in the Act will also help secure the 5G networks of the future. For example, the Act requires the FCC to "develop of list of suggested replacements of both physical and virtual communications equipment, application and management software, and services or categories of replacements of both physical and virtual communications equipment, application and management software, and services." Applied in a neutral fashion, this list can provide guidance to all carriers regarding secure equipment options for current and future network deployments, including end-to-end equipment used by most carriers today as well as increasingly virtualized and open source equipment and services.

As 5G wireless services provide increased potential to transfer network services from physical equipment to software, new technologies are increasingly coming to the market, including Open Radio Access Network ("ORAN") equipment. ORAN presents exciting new opportunities, with the potential to disaggregate functionality to increase efficiency and reduce costs. I encourage further research and development to explore virtualized solutions. ORAN may provide opportunities to increase security by breaking down the network stack and allowing multiple vendors to provide off-the-shelf components and services that when working together appropriately provide unified services. The potential for introducing American vendors into the ecosystem has tremendous benefits, but each layer must be sufficiently vetted for security. Particularly in greenfield network builds, ORAN can provide opportunities for new network designs that do not need to be integrated to legacy networks. For example, DISH, a CCA member, has announced plans to start deploying its standalone ORAN 5G network this year in the United States.

However, policymakers should not mandate which technologies are used in wireless networks, but instead should encourage research into new, secure technologies to enhance customer choice, innovation, and cost savings. For carriers with existing network infrastructure, additional research may facilitate increased ORAN deployment as well, and it is important that all network operators are positioned to manage additional steps for interoperability across multiple vendors. Absent a secure deployment approach, the increased number of access points that can present opportunities for additional vendors can expose additional entry points for bad actors. While ORAN equipment may be designed for network efficiencies, these technologies are not necessarily designed with the specific goal of enhancing security.

If new technologies like ORAN are successful, they will compete successfully in the marketplace. We must be mindful, however, that mandating using specific technology could require additional time for carriers seeking to replace covered elements from their networks, presenting a question of competing goals for policymakers. Smaller providers often rely on one or a small number of equipment providers for end-to-end services and do not have regular access to expansive test beds to vet all network elements. Carriers will continue to rely on existing trusted vendors, and may not be prepared for interoperability and system integration costs involved with multiple providers. They can ill afford to discover errors after deployment and operations are turned up to provide service and may have additional burdens to determine the cause of an error if there is a service outage. Further, smaller carriers depend on shared economies of scale for equipment with their larger competitors and are not in a position to drive the ecosystem. As previous technologies have been deployed at scale, smaller carriers can obtain economical access after deployment by larger carriers. Some smaller competitive carriers have also expressed concerns that an exclusive focus on new technologies that are not yet fully standardized or vetted could risk cannibalizing existing, trusted equipment providers.

As we seek to advance technologies and innovate, policymakers must ensure that the United States telecommunications industry does not lose access to trusted suppliers in the pursuit of potential new and exciting technologies of the future.

Additionally, I applaud inclusion in the legislation the creation of an information sharing program, led by the National Telecommunications and Information Administration and in cooperation with several other leading agencies, to share information regarding supply chain security risks with trusted communications providers and suppliers. This program can help ensure that all stakeholders have the information they need to continue to make decisions to secure networks into the future.

* * * * *

In closing, I would like to again congratulate this Committee for its leadership in passing the Secure and Trusted Communications Networks Act. As it is implemented, CCA is committed to working with Congress, the Administration, and all stakeholders to accomplish the unprecedented task of removing certain equipment out of telecommunications networks and ensuring network operations proceed using trusted vendors, all while maintaining communications services for millions of Americans in rural areas. Building upon these efforts to secure existing networks, we also have an opportunity to ensure that security is a pillar of 5G networks as they expand throughout our Nation.

Thank you for the opportunity to testify at this important hearing, and I welcome any questions.

The CHAIRMAN. Thank you very much, Mr. Berry.

Mr. Boswell.

STATEMENT OF JASON S. BOSWELL, HEAD OF SECURITY, NETWORK PRODUCT SOLUTIONS, ERICSSON NORTH AMERICA

Mr. BOSWELL. Thank you. Chairman Wicker, Ranking Member Cantwell, members of the Committee, thank you for the opportunity to appear today on behalf of Ericsson.

I'm Jason Boswell, Ericsson's Head of Security for Network Product Solutions in North America. Since my early days as an engineer, I've spent my whole career focused on security and advanced telecommunications, and I'm pleased to provide Ericsson's perspective on 5G supply chain security.

Let me start by commending the recent passage of Chairman Wicker's bipartisan security legislation, The Secure and Trusted Communications Networks Act.

We stand ready to assist small carriers replacing equipment from untrusted vendors. The U.S. led the way on 4G and reaped the economic benefits, $475 billion to GDP and four million U.S. jobs. 5G will accelerate innovation and deliver even more transformative benefits to consumers and businesses alike with the potential to bring $500 billion to the U.S. economy and three million new U.S. jobs.

But this also brings new security challenges due in part to the increased potential attacks surface. We need networks that are trustworthy, resilient, and secure by design, enabled by a robust market of trusted suppliers, not just in the United States but worldwide.

Ericsson is leading the way on secure 5G, supporting 65 percent of the 5G deployments across the U.S., including in rural America. We have customers in over 180 countries, and I'm proud to say that the U.S. is our largest market, accounting for 30 percent of our global revenue and driving our R&D priorities.

Ericsson has a longstanding and expanding commitment here. Our North American headquarters is in Plano, Texas, and we currently have over 7,000 employees in the U.S. We also have a tower technician training facility in Texas and we will soon open our $100 million 5G Smart Factory right here in the U.S.

In fact, in some breaking news, this just came in this morning, today we announced our first 5G equipment rolling out from that factory manufactured right there in Lewisville, Texas.

Security is intertwined with the successful deployment of 5G networks and three key priorities will enable this 5G rollout. First, we need increased mid-band spectrum availability and we commend the FCC for allocating some mid-band spectrum for 5G. It is a good start but more is needed.

Second, we need streamlined rules for small cell siting as provided in Senators Thune and Schatz's STREAMLINE Act.

And third, we need to focus on developing a skilled 5G workforce. Senators Gardner and Sinema's Tower Infrastructure Deployment Act and Senators Thune, Tester, Moran, Peters, and Wicker's Telecommunications Skilled Workforce Act would do just that.

Security is a top priority for Ericsson and our actions reflect our philosophy, both internally and externally.

First, since 2018, we have been executing a supply chain regionalization strategy to place manufacturing and development as close to the customer as possible in order to reduce risks, regional disruptions, and dependence on one supply site or vendor, and in all of our manufacturing and software development, Ericsson secures our own supply chain with integrity checks, site audits, sign-in and sign-out for all software development, and cryptographic signing of hardware and software that helps provide routes of trust for all of our portfolio.

Second, we take a holistic approach to building security into our systems from the start. Our own security and reliability model guides security assurance across all of our products and helps inform standards development.

Third, we lead industry-wide endeavors to advance security across the whole 5G ecosystem, not just Ericsson products. This involves our standards activities and also the development of best practices for 5G security. We are active on the DHS Supply Chain Risk Management Task Force where I co-chair a working group on developing the standardized template for supply chain evaluation to minimize risk in the purchasing process.

I'm also a member of the FCC's Security Advisory Committee. I am on a working group focused on managing security risk in the transition to 5G.

We need to sustain a secure and robust marketplace of trusted suppliers in the U.S. and globally. To do so, it is important to continue to pass 5G security legislation, such as the thoughtful bill pending from Senators Cornyn, Sullivan, Blackburn, and others, and keep holding hearings like this one to highlight what industry and government agencies are doing to ensure a secure 5G ecosystem.

Shining light on these efforts will make them even more effective and allow the U.S. to set the global example for 5G security.

On behalf of Ericsson, I thank the Committee for its leadership. We look forward to working with you and I look forward to your questions.

[The prepared statement of Mr. Boswell follows:]

PREPARED STATEMENT OF JASON S. BOSWELL, HEAD OF SECURITY, NETWORK PRODUCT SOLUTIONS, ERICSSON NORTH AMERICA

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for the opportunity to appear today on behalf of Ericsson and to share our views on the important subject of supply chain security in the 5G world. Ericsson commends the Committee for its focus on these important issues, and we welcome the recent passage of Chairman Wicker's bipartisan Secure and Trusted Communications Networks Act. As Head of Security for Network Product Solutions in Ericsson North America, I advise Ericsson's technicians, engineers, partners, and customers on creating and maintaining secure Ericsson solutions across the country. I also represent Ericsson in numerous industry initiatives and collaborative efforts with government to develop and implement industry-wide practices and policies to make the 5G supply chain trustworthy, resilient, and secure. Since my early days as an engineer more than 20 years ago, I have spent the entirety of my career focused on security and advanced telecommunications. I am pleased to be able to describe Ericsson's perspective on the important topic of securing 5G and its supply chain.

I. Introduction

A Pivotal Moment for 5G. 5G will accelerate innovation, enhance productivity, and make our lives better through transformative use cases in manufacturing, telemedicine, agriculture, connected cars, smart cities, and the Internet of Things, to name a few, plus a host of applications and services that are still to come. 5G will deliver significant benefits to consumers and business alike.

But this innovation brings new security challenges for the mobile ecosystem as well, with broader attack surfaces, more devices, and greater traffic. The United States is expected to account for 50 percent of the data breached or compromised across the globe by 2023—we will be the lead target for cyberattacks. This is a clear call to action for the U.S. We need networks that are trustworthy, resilient, and secure by design—all on day one.

In short, as we embark on the 5G future and usher in the next decade of telecommunications, we face a series of critical decisions, and we have an opportunity for the U.S. to set a global example in 5G network security across policy, technology, and standards. Whether we live up to this moment will depend on how industry and government together answer these questions:

- Will 5G be innovative and dynamic?
- Will 5G be secure and reliable?
- Will 5G support the rule of law and enable fair competition and the robust marketplace necessary to protect national security?

I believe that with intentionality and foresight, the United States will provide an emphatic "yes" in response to each of these questions. This morning, I will share Ericsson's perspective on key priorities and key action items that will help guide us through this moment.

Ericsson: Who We Are and What We Do. At Ericsson, we long ago embraced the idea of making communications available for everyone, and we have aggressively executed on that vision ever since. Today, we serve customers in the United States and more than 180 other countries.

Ericsson is a global 5G leader. To highlight just a few accomplishments:

- We were the first supplier with commercial 5G live networks in four continents, and currently we support twenty-four live 5G networks in fourteen countries.
- We now support the widest ecosystem of supported devices on 5G live networks, with over forty.
- In every nation state that has conducted a national security 5G assessment, Ericsson has been designated as both a secure and trusted 5G supplier.
- Since 2015, we have delivered more than five million 5G-ready radio units world-wide, which only need a remote software update to launch 5G; hypothetically, this number of radios corresponds to covering the entire U.S. and Europe with 5G.
- We led the way on 5G standards, with the highest share of 5G essential patent declarations—15.8 percent—of any organization in the world. And more broadly, we have one of the industry's strongest intellectual property portfolios, which includes more than 54,000 granted patents worldwide. Ericsson is the largest holder of standard essential patents for mobile communication. Our unrivalled

patent portfolio covers 2G, 3G, and 4G, and we are the main driver of industry standardization for 5G.

Our primary headquarters is in Sweden—a country with which the U.S. has a longstanding defense cooperation—but we have key development operations, as well as product, verification, and release activities, in North America. The United States is our largest market, and Ericsson has a longstanding and expanding commitment to the U.S. Our presence in the U.S. dates back nearly 120 years. Ericsson now has over 7,000 employees working in the U.S., and our North America headquarters is located in Plano, Texas. And, we are actively expanding our investment in U.S. manufacturing and U.S. jobs. Of note, we are opening our first 5G smart factory in the United States, in Lewisville, Texas. This facility will be a connected smart factory, producing Advanced Antenna System radios to enable rapid 5G deployments. In addition, our Lewisville, Texas Center of Excellence (CoE) is an enhanced tower technician training facility that provides best-in-class field services training and support for Ericsson's employees and partners. In 2019, 847 tower tech trainees completed training at the Lewisville CoE.

Over the last two years, Ericsson has had other investments and achievements in the United States, including:

- Producing the first 5G radios in the U.S. in 2018, with a production partner in St. Petersburg, Florida;
- Supporting 65 percent of the 5G deployments across the United States, including efforts to close the digital divide in rural America;
- Opening a 5G ASIC Design Center in Austin, Texas, to help accelerate 5G product development; and
- Creating a new innovation hub at Ericsson's Silicon Valley facility in Santa Clara, California to enable our industry partners and customers to accelerate adoption of advances in artificial intelligence (AI) and machine learning.

Apart from its direct investments in the U.S., Ericsson serves a broad and diverse U.S. customer base, which includes nationwide and regional communication service providers serving both rural and urban markets with all technologies (wireline and wireless telecommunications, cable, and satellite). We have partnerships and collaborations with rural Wireless Internet Service Providers (WISPs) and carriers—such as GCI Communications, Cellcom, Bluegrass Cellular, and many more—in furtherance of our commitment to bring 5G to rural areas. Ericsson also maintains strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies. In fact, Ericsson's global sourcing of active components for Ericsson's 5G radio base stations relies up to 90 percent on U.S. technology suppliers. Finally, we participate in more than 100 industry organizations, standards bodies, and other technology alliance groups.

As discussed further below, Ericsson employs a holistic approach to ensuring the security of its supply chain and its products, which is made more effective by an environment here in the U.S. consisting of pro-deployment public policies and 5G investment, combined with industry-led collaboration with government for a secure 5G ecosystem.

II. Ericsson's View of the Priorities That Enable a Successful and Secure 5G Rollout

Security is inextricably tied to the successful development of 5G networks—without one, you simply do not have the other. Before explaining Ericsson's approach to assuring 5G supply chain security, let me identify three key priorities for enabling a successful and secure 5G rollout.

Accelerating 5G deployment in North America. The United States enjoyed first mover advantage in the 4G world, and it can win the 5G pole position as well. Indeed, the North American market is large enough to lead the world market, setting the global agenda for innovation and security and market competition. Conversely, any delay in 5G advancement policies could allow other actors that may pose national security risks to gain the first-mover advantage in the 5G investment cycle and set technology standards for global companies to adopt. In short, being first in 5G deployment is not merely an honorarium—it is a meaningful step toward a secure 5G ecosystem.

As Ericsson has advocated, and as the members of this Committee have advanced, Congress can accelerate 5G deployment in the U.S. by taking the following near-term actions:

- Increase spectrum availability, especially mid-band;
- Put in place reasonable, streamlined small cell siting rules;

- Develop and deploy a skilled tower workforce; and
- Ensure effective incentives to encourage 5G deployment in rural areas.

Below, I identify several measures before the Senate that can help accomplish these objectives.

Strengthening and ensuring the long-term viability of a competitive, dynamic, diverse, robust global market of trusted and secure suppliers. Over the past two decades, the global market of wireless communications equipment suppliers has seen significant consolidation, but today there are a number of suppliers of 5G radio access network equipment in addition to Ericsson. Additional suppliers, including U.S. companies, provide different elements of core network equipment, and evolving innovations in open and interoperable networking and virtualization will allow new participants to compete with established global suppliers. In short, even with bans on Chinese vendors, the 5G ecosystem presently is diverse and competitive—attributes that are imperative not only for ever-advancing innovation but also to ensure security and resiliency throughout global networks.

A key strategic goal for public policy aimed at a secure and trusted 5G supply chain is to maintain a global, competitive, diverse market of trusted suppliers. Network security is a global issue, not just a domestic one, and security on a global level only reinforces and enhances security here at home. We should therefore continue to encourage the adoption, without delay, of principles and guidelines favoring trusted suppliers and supply chains—on a *global* basis. We all have a mutual interest in such a competitive market—suppliers and service providers alike. And we agree with the principles that security and trust are two independent factors that need to be assessed to protect 5G networks. These principles are key to establishing an end-to-end view of risk across the multiple layers of telecommunications infrastructure.

Supporting the important, ongoing work of standards processes and government-industry coordination. Ericsson is a leading participant in developing the standards for 5G security through the global 3rd Generation Partnership Project (3GPP), and we are engaged in an effort through the Alliance for Telecommunications Industry Solutions (ATIS), supported by the Department of Defense, to develop standards for securing the 5G supply chain. These technical standards are crucial for security because they give all suppliers and carriers a common—and open and transparent—technical understanding of interoperability and security. This allows for vetting and identification and correction of technical vulnerabilities. To be clear, 5G security standards and 5G supply chain standards are presently still under development, and Ericsson is helping shape them for long-term security.

Once industry adopts standards, the next crucial step is effective network configuration and deployment. Here, I need to emphasize how 5G is different from previous generations of wireless communications. Unlike the steps from 1G to 2G to 3G to 4G, each of which constituted advances in both capability and security, 5G is a totally new and different technology and network architecture. When fully deployed, 5G will be "virtualized" across a service based architecture (SBA)—meaning that the core network functions will happen through a cloud-based and "software defined" network, which allow tailored security solutions for each different network function, also known as a network "slice." Virtualized networking will allow for unprecedented capabilities for specialization in security for different isolated functions—for instance, separating mission-critical network instances such as connected medical devices from less critical devices and functions. These new architectures and technologies will also allow for more discrete control of access to data, topology obfuscation between network segments, greater requirements on inter-element encryption, provisions for extended authentication, enhanced privacy protections for subscribers, and many other new capabilities. Individual configurations in real-world deployments will be different in every case, but in all cases they should be based on the rigorous, open, and interoperable standards that Ericsson is helping develop now.

We believe the role of the government in advancing the security of these deployments is to continue to put its attention and resources behind the robust government-industry collaboration efforts that are presently underway. In short, we must work together effectively and efficiently to ensure that these deployments are secure, as described below.

III. Ericsson's Activities and Leadership That Advance These Priorities

Security is a top priority for Ericsson, and our actions on security reflect our philosophy: Networks must, from the very start, be trustworthy, resilient, and secure by design.

How does Ericsson ensure a secure supply chain? In all of our manufacturing and software development facilities globally, Ericsson relies on tight quality controls, traceability and integrity checks, regular site audits, tests, and verifications to ensure compliance with our own security standards and appropriate industry specification guidelines. All of Ericsson's software is verified, cryptographically signed, and distributed centrally from Sweden, and, when so required, under Swedish export licenses. We have strict software version controls with check-in/check-out security, meaning that both the Ericsson employee who wrote the code and the individual who reviewed/accepted the changes are logged. Binaries are provided via secure download from the Ericsson Software Gateway in Sweden, including a signature which provides a trust anchor that ensures the software originated from Ericsson and has not been tampered with in transit.

Where are Ericsson products developed and manufactured? Ericsson has a global, flexible, high-integrity supply chain, with manufacturing established in several countries around the world—including a sizeable presence in the U.S., as I described above. Since 2018, we have been proactively 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. In general, all active "intelligent" 3PP 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.

How does Ericsson provide security assurance? Ericsson takes a holistic approach to ensure that security is built in from the start, across supply chain, software and hardware development, testing, implementation, and operation. For many years, Ericsson has worked systematically to incorporate security from the start (security by design) into all phases of product development, and we have a well-established internal governance framework for product security. This framework is how Ericsson is able to consistently deliver on our product security commitment. The framework's key characteristics include:

- Defining our product security and privacy ambition level;
- Ensuring the implementation of appropriate security and privacy;
- Following up and measuring actual product security and privacy status; and
- Enabling professional security services, such as security and privacy training recommendations, solution level integration guidance, and potential hardening activities that need to be included in customer delivery projects.

In addition, all personnel and suppliers follow Ericsson's Code of Conduct and Code of Business Ethics. 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 and ISO 9001, which are recognized as international guidelines on Information Security Management and requirements for Quality Management Systems, respectively.

Finally, we strongly believe in the principles of responsible vulnerability disclosure towards all parties involved. Accordingly, the Ericsson PSIRT (Product Security Incident Response Team) is responsible for our product vulnerability management process, coordination of customer product security incidents, and reported security issues affecting Ericsson products, solutions, and services.

How does Ericsson promote and advise on industry-wide best practices in 5G and supply chain security? Our security efforts do not end with our products—Ericsson actively contributes to a number of U.S.-based industry initiatives organized around ensuring supply chain security. These include the Communications Sector Coordinating Council (CSCC) and its Cybersecurity Committee (where I participate directly as a member), the Council to Secure the Digital Economy (CSDE), and multiple working groups within the standard-setting organization ATIS.

I also personally provide leadership in numerous government-industry initiatives convened to promote collaboration on supply chain security. I will cite three examples here, which are especially relevant to this discussion.

First, it has been my privilege to participate in the groundbreaking work of the Department of Homeland Security (DHS) Information and Communications Technology (ICT) Supply Chain Risk Management Task Force. The DHS ICT Supply Chain Risk Management Task Force exemplifies how industry and government collaboration can quickly and effectively deliver useful, sharable, expert-driven guidance in complex areas like supply chain and 5G security. The Task Force represents a formal, action-oriented collaboration between industry and government that ties together various streams of activity. For example, in September 2019, the Task Force released an interim report with findings and recommendations from working groups that focused on:

- The timely sharing of actionable information about supply chain risks across the community (WG1);
- The understanding and evaluation of supply chain threats (WG2);
- The identification of criteria, processes and structures for establishing Qualified Bidder Lists (QBL) and Qualified Manufacturer Lists (QML) (WG3); and
- Policy recommendations for incentivizing the purchase of ICT from original equipment manufacturers and authorized resellers only (WG4).

In 2020, I will continue Ericsson's work in the Task Force Threat Evaluation Working Group (WG2) by analyzing mitigations and risk determination across multiple areas of the supply chain and making recommendations on best practices and methodologies. I will also be co-chairing a new working group (2020 WG4) to develop attestation frameworks around various aspects of supply chain risk management. This will help make requirements such as the NIST security standards and other risk guidelines more understandable, predictable, and useful, and also will address gaps in risk management or visibility by providing a flexible template that can help guide planning and assessments and provide clarity for acquisition reporting and vetting processes.

Second, I participate in the important work of the President's National Security Telecommunication Advisory Council (NSTAC). In particular, I serve on a subcommittee tasked by the NSTAC with examining the security impact of software-defined networking (SDN) on the U.S. government's National Security and Emergency Preparedness functions, identifying the challenges and opportunities provided by SDN, and assessing the use of SDN and other virtualization technologies in support of national security.

Third, I represent Ericsson on the Communications Security, Reliability, and Interoperability Council (CSRIC), which makes security policy recommendations to the Federal Communications Commission (FCC). Ericsson is working across three working groups in the current iteration of CSRIC, CSRIC VII, notably:

- Managing Security Risk in the Transition to 5G (WG2), in which I am directly involved;
- Managing Security Risk in Emerging 5G Implementations (WG3); and
- 911 Security Vulnerabilities during the IP Transition (WG4).

Beyond these activities, we also work closely with other government departments and agencies, including the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST), both within the Department of Commerce, as well as with the Departments of Defense and Energy.

Standards work is another foundational component of good security assurance, as it supplies guidance and frameworks that ensure security and privacy requirements are met consistently. Ericsson has been a leading contributor in standards and frameworks groups such as 3GPP, ETSI, IETF, GSMA, IEEE, the O–RAN Alliance, the Open Network Foundation, and many more. As noted above, in total, Ericsson is a member of more than 100 industry organizations, standards bodies, and other technology alliance groups, as part of our mission to drive 5G forward.

IV. Ericsson's Recommendations for the Committee to Support and Promote These Priorities

At the beginning of my testimony, I listed three questions that mark this moment in the trajectory to 5G:

- Will 5G be innovative and dynamic?
- Will 5G be secure and reliable?
- Will 5G support the rule of law and enable fair competition and the robust marketplace necessary to protect national security?

As noted above, I believe that with intentionality and foresight, the answer to these questions can be an emphatic "yes." Now for the hard part: How do we get there?

As a general matter, Ericsson urges the Committee to support the various efforts described above, with an eye toward ensuring that industry and government are coordinating efficiently and collaborating productively on 5G security and supply chain matters, both domestically and globally.

More specifically, we recommend that the Committee take the following steps:

(1) *Pass, implement, and oversee 5G security legislation.* As I noted at the outset, the Senate's recent passage of Chairman Wicker's Secure and Trusted Communica-

tions Networks Act represents a thoughtful and crucial step forward. We look forward to the President signing this bill and stand ready to work with the small operators who will have to replace existing equipment. As the Committee is well aware, further opportunities to build on the momentum of that legislation await, as several additional bipartisan 5G security-related bills have passed in the House of Representatives. These include the House companion bill to Senator Cornyn's Secure 5G and Beyond Act, co-sponsored by Senators Sullivan and Blackburn of this Committee and others, which would require the U.S. to develop a 5G security strategy. Passage of such measures in the Senate would help demonstrate the U.S. commitment to 5G security to countries around the world grappling with these issues.

(2) *Support actions to accelerate 5G deployment.* As I discussed, Ericsson believes that accelerated U.S. 5G deployment will in turn protect the security of the 5G supply chain, a goal that can be achieved through (i) increasing spectrum availability, especially mid-band; (ii) putting in place reasonable, streamlined small cell siting rules; (iii) developing and deploying a skilled tower workforce; and (iv) ensuring effective incentives to encourage 5G deployment in rural areas. We commend the work being done in these areas and urge the Committee to take up proposals to advance 5G deployments in the U.S., such as the STREAMLINE Act introduced by Senators Thune and Schatz, which would preempt certain state/local small cell deployment regulation; the TOWER Infrastructure Deployment Act introduced by Senators Gardner and Sinema, which would require the FCC to set up an Advisory Council to look at tower workforce issues; and the Telecommunications Skilled Workforce Act recently introduced by Senators Thune, Tester, Moran, Peters, and Wicker, which would require cooperation among various agency heads to develop recommendations and guidance that would empower the U.S. to catch up on the workforce demands of the 5G era.

(3) *Continue to enable a secure and robust marketplace of trusted suppliers in the U.S. and globally.* As I have discussed, one of the key priorities for 5G is to strengthen and ensure the viability of a competitive, dynamic, diverse, and robust marketplace of trusted and secure suppliers on a global level, much like what we already have in the United States, recognizing that global and domestic security are intertwined. Such a marketplace, involving trusted and secure companies like Ericsson, can counter other potential players that may pose threats to national security. The Committee should remain attentive to factors that might promote—or undermine—the development of this global marketplace.

(4) *Continue to hold hearings on the subject of 5G security.* In Ericsson's view, hearings such as this one provide an important vehicle for highlighting what industry is doing to ensure a secure 5G world—and for maintaining pressure on industry to stay true to its security commitments. Such hearings can have a similar motivating impact on government actors with security responsibility within their respective jurisdictions around the world. Shining additional light on all of these efforts will make them more effective in ensuring a secure supply chain.

* * *

On behalf of Ericsson, I thank the Committee for its leadership in this area. We look forward to continuing to work with you, other government actors, and our industry partners to ensure that the 5G world is a secure one. Thank you again for the opportunity to testify today, and I look forward to your questions.

The CHAIRMAN. Thank you very much, Mr. Boswell.

Ms. Keddy.

STATEMENT OF ASHA KEDDY, CORPORATE VICE PRESIDENT AND GENERAL MANAGER, NEXT GENERATION AND STANDARDS, INTEL CORPORATION

Ms. KEDDY. Chairman Wicker, Ranking Member Cantwell, and members of the Committee, thank you for inviting me to speak about 5G and supply chain [off microphone comments] Intel Corporation.

My responsibilities include our participation in industry standards and forums, including 3GPP, and driving the benefits of 5G to various other industries to fuel widespread innovation.

Intel is a U.S. semiconductor manufacturer that employs more than a 100,000 people globally with more than half of those in the

United States. Intel is the largest global semiconductor supplier with the vast majority for advanced manufacturing and R&D conducted in the U.S.

It used to be Intel inside only in computers, PCs, and data centers, but now we are inside the network, as well. 5G runs on Intel. We are a leader in 5G and one of our roles is to supply high-volume and high-quality products to telecom equipment manufacturers, including Nokia and Ericsson.

By 2021, we are expected to become the world's largest chip maker for 5G infrastructure. Intel takes a leading role in 5G standards and industry groups, including 3GPP, IEEE, and ITU. I also represent Intel at CTIA's Board of Directors and Intel is a member of the ORAN Alliance and the new ATIS 5G Supply Chain Working Group.

For today's discussion on 5G supply chains, I would like to begin by discussing current developments regarding 5G networks followed by our work to improve supply chain security and some policy recommendations.

5G marks the convergence of communications and compute capabilities which will fundamentally change our world. The U.S. was the first nation with widespread 4G coverage which led to the American app economy. 5G will enable benefits to businesses in many sectors, such as industrial and IOT manufacturing, transportation, agriculture, and health care.

Virtualization is critical to enabling the transition to 5G. As a part of this evolution, some of the network functions are being virtualized rather than being served by a turnkey solution, creating what we call a virtual radio access network or VRAN.

Intel's product line supports various 5G network approaches ranging from the traditional telecommunications equipment manufacturers, like Ericsson and Nokia, so that they can continue to develop products to ensure continuity in the telecom industry to also new VRAN entrants, such as Altiostar and Mavenir.

We recognize that security challenges exist. Intel will continue our proactive efforts to build a more trusted foundation for all computing systems. Intel's unique position in the technology supply chain has allowed us to take a leading role when it comes to transparency and security in partnership with our suppliers and customers.

We have already developed a set of policies and procedures at our own factories to validate where and when Intel-built components were manufactured.

In today's complex supply chain for information and communications technology, Intel is working with manufacturers across the supply chain to help them offer customers better transparency and visibility into manufacturing, support, and retirement of computing devices. Intel calls this effort Compute Lifecycle Assurance.

The industry needs an end-to-end framework like this initiative that can be applied to improve integrity, resilience, and security during the entire platform cycle.

The U.S. Government also has a valuable role to play in the 5G supply chain by encouraging and supporting the emergence of a vibrant and trusted U.S. ecosystem. Given the potential of 5G to provide valuable benefits to American businesses and consumers, the

U.S. Government should take measures, including investments and incentives, to help facilitate widespread 5G deployments in the U.S. and to accelerate new technological innovation.

Thank you for the opportunity to highlight Intel's role in this 5G ecosystem and our approach to supply chain security. I look forward to your questions.

[The prepared statement of Ms. Keddy follows:]

Prepared Statement of Aysha Keddy, Corporate Vice President and General Manager, Next Generation and Standards, Intel Corporation

Chairman Wicker, Ranking Member Cantwell, and Members of the Committee, thank you for inviting Intel to speak about 5G supply chain security. I serve as Corporate Vice President in engineering, responsible for next generation technology and standards at Intel Corporation. In this role, I am responsible for future products including the convergence of communications, compute and artificial intelligence and defining the future networks towards 6G. My responsibilities also include Intel's contributions to industry standards and the company's leadership in global forums including IEEE, 3GPP and multiple industry fora. It is my job to drive the benefits of 5G to various other businesses by fueling innovation for homes, cities and enterprise.

Intel Corporation is a U.S. semiconductor manufacturer headquartered in Santa Clara, California that employs over 100,000 people globally, with more than half of those in the United States. Intel is the largest global semiconductor supplier, with the majority of our advanced manufacturing and research and development (R&D) is conducted in the United States. Revenue earned in global markets contributes to Intel's Annual R&D and Capital Investments of 29.6 billion dollars.[1] Intel is one of the last integrated device manufacturers (IDM) in the United States. This means Intel owns production for most of its products from conception, through design, to manufacturing, all the way to delivery to a device manufacturer. Having most of our design and fabrication within the same company creates significant technology advantages for Intel in setting the highest standards for quality, consistency and security. And when we identify problems, the IDM model creates advantages for Intel in resolving problems rapidly.

Intel's processors, memory, storage and other products power much of the world's computing capability. Intel is a leader in 5G and one of our roles is to supply high volume and high-quality products to telecom equipment manufacturers. By 2021, we are expected to become the world's largest silicon provider for 5G infrastructure. 5G runs on Intel. It used to be Intel inside computers and data centers, but now Intel is inside the network as well.

Intel also participates in over 250 standards and industry groups worldwide including industry alliances, regional standards organizations, international industry standards groups and formal international standards bodies. For 5G standards involvement, Intel holds leadership positions in 3GPP, IEEE, and the International Telecommunications Union. Intel is also a board member of the Telecom Infra Project and a member of the ORAN Alliance. Intel also participates in the new ATIS 5G Supply Chain Working Group tasked by the Department of Defense with developing standards and evaluating certification options necessary to establish "assured" commercial 5G networks.

For today's discussion on 5G supply chains, I would like to begin by discussing some developments regarding 5G networks followed by some important considerations regarding supply chains.

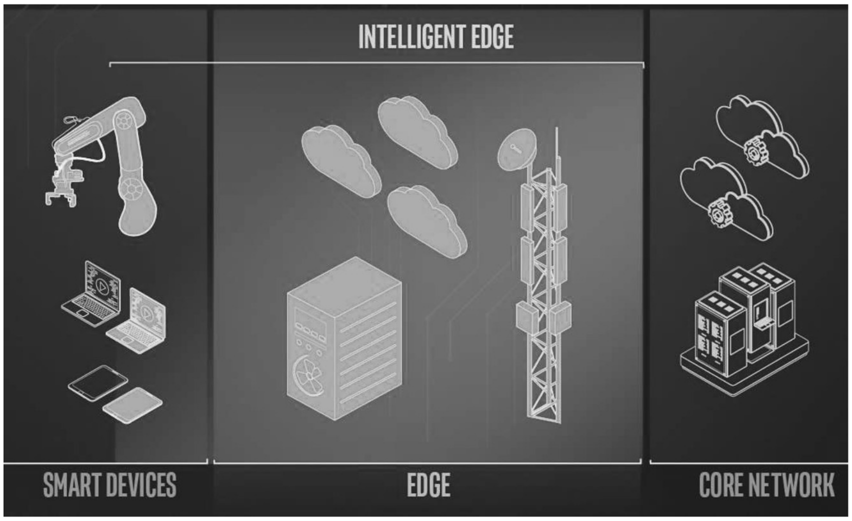
5G networks:

5G marks the convergence of communications and compute capabilities, a world in which 5G, Wi-Fi, artificial intelligence, the cloud, and edge computing combine to fundamentally change our world. The U.S. was the first nation with widespread 4G coverage which led to many innovations that many of us use every day on our smartphones from ordering rides to groceries to take-out dinners to checking in for flights to reading books or watching shows. 5G will enable these types of benefits to businesses in many different industries such industrial IoT in manufacturing, mining, agriculture, healthcare, etc.

[1] Source: 2019 Q4 10K filing from Intel Corporation, *https://www.intc.com/investor-relations/financials-and-filings/earnings-results/default.aspx*

Virtualization is critical to enable to transition to 5G. Radio Access Network (RAN) architectures are evolving to support a diverse set of deployments. As part of this evolution, some of the network functions are virtualized rather than being served by discrete products, creating what are called virtual Radio Access Networks. An analogy would be if you previously needed one computer to do presentations, another computer to browse the internet, another computer for e-mail, etc. but now you can do all those functions on a single computer. This way you can use the processing power on the application that needs it the most at a specific point in time.

Network virtualization has been a ten-year journey across the communications industry, which started at the core of the network to service provider metro and neighborhood central offices—and now out to the RAN, the last link between users and the network (*e.g.,* cell tower to end user). Network virtualization enables the agility of software-based innovation. Just as this approach enabled the dot com companies of the 90s to provide new services to consumers, software innovation including Virtual RANs are intended to enable a breadth of service opportunity in telecommunications.



3GPP is developing a global 5G standard which will be implemented in networks worldwide. These networks will include traditional cellular operators as well as new entrants. Different services providers will take steps in network virtualization on varying timelines, so different options will exist ranging from the traditional telecommunications equipment manufacturer model to the different flavors of Virtual RAN. Open RAN, such as the work within the Open RAN Alliance, is one version of a Virtual RAN. The Open RAN Alliance is working to develop an interoperable specification with open interfaces between the base stations and the radio which enables cellular operators to utilize different vendors.

Intel's product lines support the various approaches ranging from traditional telecom equipment manufacturers (*e.g.,* Ericsson and Nokia), so they can continue to deliver products to ensure continuity in telecom industry, to new entrants (*e.g.,* Altiostar and Mavenir) through our rich software development kit, open source activities and reference platform designs.

Technology Supply Chains

We recognize there are security challenges to overcome. Worldwide, policymakers have begun to focus on supply chain risks in new ways. In August 2018, MITRE published the highly influential report, Deliver Uncompromised, which described the urgency and importance for supply chain risks to receive attention during product procurement. New U.S. laws, including the 2018 SECURE Technology Act, gave Federal agencies new authority to consider supply chain risks when procuring products. From Europe's "digital sovereignty" efforts to Japan's "Cyber/Physical Security Framework" efforts, there are signs of strong interest in shining a spotlight on the trust and transparency of supply chains for information and communications technology.

Intel will continue our proactive efforts to build a more trusted foundation for all computing systems. Intel's unique position in the technology supply chain has allowed us to take a leading role, in partnership with our suppliers and customers, when it comes to transparency and security. Intel's supply chain depends on successful, consistent, and trustworthy relationships with roughly 14,000 companies who provide Intel with the raw materials, products and services required for us to supply technology to over 2,100 customers. The collaboration and commitment occur across the supply chain—from Intel's suppliers, through Intel internal production, and outbound to Intel's customers.

Intel identifies four key stages in the compute supply chain: build, transfer, operate and retire. Each stage includes unique threats. Examples of these threats include:

Build

- Injection of malicious code, logic or components during design or manufacturing
- Cyber-attack against a supplier resulting in denial of service (DOS), supply chain disruption, data corruption, data breach

Transfer

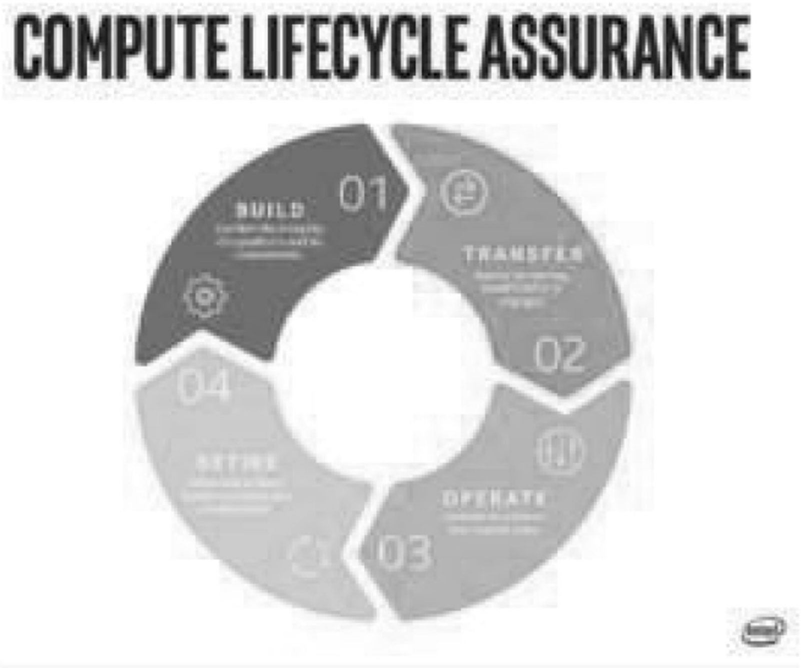
- Counterfeit for profit, sabotage, or other reason
- Interdiction and tampering during manufacturing or transit

Operate

- Compromising administrator credentials
- Installation of vulnerable code or components

Retire

- Theft of components/data from retired system
- Appropriate of residual data left on systems



Compute Lifecycle Assurance

Addressing the gap between trustworthiness and 'leap of faith' is a primary motivation for a new Intel initiative designed to help increase data available to end user customers about the supply chain that brings computing devices to your doorstep.

Intel describes the effort as “Compute Lifecycle Assurance,” and it starts with the goal of making supply chains more transparent.

Intel has tackled big, complex problems like this before. We actively led and collaborated with the industry to influence policies and processes concerning the use of conflict-free minerals—not only for Intel products—but across the industry. In addition, we have already developed a set of policies and procedures at our own factories to validate where and when every component of a server was manufactured. These examples represent an important beginning, and there is more that can be done.

In today’s increasingly complex supply chain environment, we want to provide our customers with a full range of tools and solutions that deliver assurances of integrity throughout the entire lifetime of a platform. This starts with a security-first approach to design. It continues as platforms change custody, ownership and physical location several times during their assembly, transportation and provisioning. Once operational, they may then require updates for optimal performance and security. Finally, upon retirement from service, platforms should ensure the confidentiality of data that was transmitted, erased or stored.

The industry needs an end-to-end framework that can be applied across this multiyear life of any platform. And that is our goal with the Compute Lifecycle Assurance Initiative—to substantially improve transparency and to provide higher levels of assurance that improve integrity, resilience and security during the entire platform lifecycle.

Today Intel is working to:

- Invest in tools and processes that improve the integrity of Intel computing products across every lifecycle stage, building on the Transparent Supply Chain tools we have today.
- Contribute best practices, learned from our decades of experience, for the collection, measurement, stewardship and reporting of platform data to meet our customers’ evolving needs.
- Collaborate with the ecosystem to develop innovative ways that enhance access to platform data while maintaining confidentiality of that data across the platform lifecycle.

Policy Considerations

The United States government has a valuable role to play in the 5G supply chain by encouraging and supporting the emergence of a vibrant and trusted ecosystem. Intel commends the work done in 2019 by the Department of Homeland Security’s Supply Chain Risk Management task force and sees this type of public sector-industry collaboration as vital to identifying and solving important questions about technology supply chain. Likewise, the work done by the Commerce Department’s National Institute of Standards and Technology (NIST), has been extremely helpful in creating common goals and frameworks for progress among policymakers and industry. Intel has been active in these and other efforts to offer its expertise and insight in addressing supply chain risks and mitigations.

Given the potential of 5G to provide valuable benefits to American businesses and consumers, the United States government should take measures to help facilitate widespread 5G deployments. Intel has advocated extensively for mid-band spectrum. Mechanisms to encourage increased investments in 5G infrastructure and to facilitate continued innovation throughout the 5G ecosystem will be critical. We appreciate Congressional and Executive Branch interest in areas such as potential broadband infrastructure deployment funding,), and ways to spur innovation and deployments in 5G such as the USA Telecoms Act, which serves as a good starting point for further discussion.

The CHAIRMAN. Thank you very much, Ms. Keddy.

Mr. Murphy.

STATEMENT OF MICHAEL MURPHY, CHIEF TECHNOLOGY OFFICER, AMERICAS AT NOKIA

Mr. MURPHY. Chairman Wicker, Ranking Member Cantwell, and members of the Committee, on behalf of Nokia, thank you for the opportunity to testify today.

First, a short introduction. Nokia’s been the leader in every generation of wireline and wireless communications. We have 11,000 employees in North America, across 28 sites, with five innovation hubs, including Bell Labs, the recipient of nine Nobel Prizes. We are the sole telecom supplier on the Ethisphere Honoree List recognizing the most ethical companies in 2020.

I'd like to address the FCC's decision requiring removal of equipment of certain vendors. Nokia completed 60 major swaps in the last 3 years, including the largest ever done, replacing 75,000 base stations in Verizon and AT&T networks. We know swaps.

Given the demand on crews for elevated 5G activity, rural customers might be challenged to complete their tasks in the 12 months indicated in the Secure and Trusted Telecommunications Networks Act. As such, we recommend that usage of the 6-month extension or more be granted liberally.

With respect to technology selection, we're at the confluence of 4G and 5G and thus many products now support both technologies. We believe rural carriers should be allowed to purchase those versus only like-for-like 4G systems. This would allow them to secure their networks and jumpstart 5G activities. The risk of gold-plating could be mitigated by employing like-for-like at the service level.

Also, there is a Senate bill that proposes to restrict monies for replacement on a condition of ORAN Alliance certification within 7 years. However, fully compliant ORAN products are few and immature. Putting that burden on rural carriers, the least capable of being early adopters, is perhaps unreasonable and thus a technology-neutral approach might be more appropriate.

Finally, there is some anxiety in this transition. However, the U.S. was the first country in the world to launch 5G networks, the first to utilize millimeter Wave, low-band frequencies, virtualized solutions, and more. These have been done by Nokia, Samsung, and Ericsson. So it is incorrect to suggest non-Chinese vendors cannot lead in the 5G or represent a reduction in capabilities.

As for the 5G marketplace at large, it is challenging. China has made aggressive use of its Development Bank to support indigenous suppliers. Payment terms offered, while legal, are unavailable to competitors through commercial banks.

The U.S. Export-Import Bank and the International Development Finance Corporation could potentially rebalance the situation. Also, the Chinese telecom market is massive, supporting significant R&D spend by domestic suppliers subsequently applied to foreign markets.

R&D spending support in the U.S. through the National Spectrum Consortium, the U.S. Connect, and the Senate Intelligence Committee bill are excellent. However, more could be done to support 5G product development, local use cases, and especially 6G research.

Finally, regarding 5G security, 5G will enable use cases supporting critical services across multiple industries. This makes the 5G attack surface larger than in 4G with the potential for catastrophic impacts should bad actors infiltrate networks.

This was known during the creation of 5G and actions in 3GPP standards have resolved many of the weaknesses in 4G. However, network breaches are still possible.

Nokia does not support the view that either product or geographic isolation are effective. Rather, security is best served by using trusted suppliers. For example, in Nokia, ethics and reporting of unethical behavior is mandatory for all employees and is a prerequisite for employment.

In product development, Nokia implements a design for security governance model that involves testing all products for vulnerabilities followed by structured resolution processes and rigid correction timelines. Transparency is mandatory.

It should be noted that these activities are independent of country of origin and that is my final thought. Namely, that the governance, historical behavior, ethics, and security systems implemented by companies are the true definition of trust.

In closing, thank you again, Chairman Wicker, Ranking Member Cantwell, and members of the Committee, for the opportunity to testify here today.

[The prepared statement of Mr. Murphy follows:]

PREPARED STATEMENT OF MICHAEL MURPHY, CHIEF TECHNOLOGY OFFICER, AMERICAS AT NOKIA

Chairman Thune, Ranking Member Cantwell, and members of the Committee, on behalf of Nokia, thank you for the opportunity to testify today.

Nokia appreciates the leadership of this Committee, Congress, the Federal Communications Commission (FCC), and the Administration in securing U.S. communications networks. In this testimony, I want to discuss several topics.

- First, given recent congressional action regarding the critical need to move forward in assisting small carriers with removing untrusted vendor equipment in their networks, I will outline several issues Congress and the FCC must keep in mind to ensure that the removal occurs without a negative impact on carriers and the communities they serve.
- Second, an important element of ensuring a secure supply chain for communications equipment is guaranteeing that the trusted suppliers already providing equipment to the U.S. market can compete at a global scale and on fair terms. I will share Nokia's perspective on the current global marketplace and some challenges that are the result of advantages extended to Chinese suppliers that are not available to other suppliers and how that can be mitigated to ensure a level playing field for trusted suppliers.
- Finally, I will highlight several of Nokia's leading security and supply chain activities, including design for security and supply chain validation, and why we believe they result in trustworthy networks. I will also comment on how new U.S. actions on supply chain security should recognize practical timelines to ensure execution success.

About Nokia:

Nokia is the industry's only global supplier having an end-to-end portfolio of network equipment, software, services and licensed technology. Our customers include communications service providers whose combined networks support 6.1 billion subscriptions, and our enterprise customers have deployed over 1,000 industrial networks worldwide. We transform how people live, work and communicate. We are the only telecommunications equipment provider listed in Ethisphere's 2020 Honoree list of ethical companies.

Nokia has a massive presence in North America with more than 11,000 employees, the bulk of those in the United States. We have 28 sites including five major innovation hubs of which four are in the United States: Sunnyvale, CA; Dallas, TX; Naperville, IL; and Murray Hill, NJ the site of the iconic Nokia Bell Labs, recipient of 9 Nobel Prizes. There are also two major Nokia data centers in the U.S., one in Plano, TX and the other in Chicago, IL. In addition, SAC Wireless, a Nokia subsidiary, has 21 sites in the United States. SAC offers turnkey services to support major network builds and upgrades for 4G, 5G, Small Cells and FirstNet. Those services include site selection and acquisition, engineering, construction, optimization, maintenance and end-to-end program management.

Nokia has been a leader in every generation of wireline and wireless communications to date and continues that leadership in 5G. The race to innovate never stops. In fact, even as we continue to roll out the earliest 5G networks, our work on 6G has already begun at Bell Labs.

Removal and Remediation of Equipment Provided by Untrusted Vendors in U.S. Rural Networks

Throughout the FCC's secure supply chain proceedings, Nokia provided technical input on the strengths and weaknesses of networks with respect to their inherent security and how a secure supply chain could be created by using our own company's internal governance as examples.

Now, given the FCC's decision to require removal of equipment from certain vendors, Nokia would like to offer additional perspectives on what the FCC and Congress should bear in mind before prescribing the final replacement guidelines and funding criteria. That advice, as I outline herein, is that flexibility in timing and technology neutrality will be essential if this effort is to be successful. Executed well, this effort can also help in the U.S.'s drive towards 5G leadership.

Flexibility in timing:

The FCC correctly recognized during its rulemaking process that a funded reimbursement program should be implemented before requiring recipients that receive universal service fund support to remove and replace covered equipment from their networks. Congress has taken the first critical step by passing the Secure and Trusted Telecommunications Networks Act.[1] Nokia believes that several provisions of the Act are prudent, particularly the provision granting discretion to the FCC to extend the time allowed for impacted carriers to replace covered equipment from one year, by up to an additional six months, and the directive for the FCC to remain technology neutral in establishing the list of recommended replacement equipment. The following provides some detail on why we support those provisions.

Nokia completed more than 60 major swaps in the last three years, including the largest ever done, replacing 75,000 base stations in both the Verizon and AT&T networks following our acquisition of Alcatel-Lucent and the transition to a new product platform. Those projects required removal and replacement while also maintaining service continuity and service quality. That is—and should be—the expectation of swap activities for all impacted carriers in this context. Based on those past experiences, Nokia can attest that these efforts require careful planning, are network specific, and the times required vary significantly from project to project. Network size is not the only factor affecting timelines. For example, new product variants or features may be required for unique spectrum combinations or to match customized capabilities provided by the previous vendor.

Beyond routine timelines, ongoing large 5G builds are creating a shortage of qualified tower crews. In fact, despite Nokia having the largest in-house field service team in the U.S., we still see a dearth of crews to meet 5G demands in 2020 and into 2021. Small rural markets covering vast rural landscapes with shortened climbing windows during winter months only exacerbate the issue. We appreciate the leadership of Senators Thune, Tester, Moran, Peters, and Wicker in introducing the Telecommunications Skilled Workforce Act to help address this gap.

In short, our view is that flexibility in timelines are a necessary practical reality, and thus extensions to the current one-year proposal will likely need to be granted liberally.

Flexibility in technology:

During the rulemaking process, the FCC proposed "to make available reasonable replacement costs for the equipment and services produced and provided by covered companies. . . ."[2] and asked whether recipients of universal service funding should be "allowed to seek reimbursement for technology upgrades to their networks . . ."[3] Nokia noted to the FCC that carriers replacing equipment need to have the freedom to buy solutions that are not just "like for like," due to the unique times we are in (that is, in the midst of a 4G to 5G transition, the drive towards more open systems and virtualization). All of these play a role in what a rural carrier should, or should not, do in removing and replacing a supplier. The following provides Nokia's recommendation on these competing and complex topics.

[1] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* Report and Order, Further Notice of Proposed Rulemaking, and Order, WC Docket No. 18–89, FCC 19–121, ¶122 (rel. Nov. 26, 2019) ("*Order and FNPRM*").

[2] *Id.* ¶137.

[3] *Id.*

Regarding "like for like," Nokia is and will continue to offer such solutions to all impacted carriers when they are available, appropriate and cost-effective. However, a significant part of Nokia's portfolio sold today supports both LTE and 5G through software upgrades. Replacing impacted carriers' equipment with older generation "LTE only" hardware could burden rural communities with avoidable near-term high 5G upgrade costs. A potential way forward is to offer "5G Ready" hardware but costing only the LTE components. Putting it another way, supporting "like for like" at the service level, but not necessarily at the hardware level. This would help mitigate the risk of gold plating and potentially help accelerate 5G in rural communities, thus supporting the U.S. drive towards nationwide 5G leadership. In short, there are no downsides.

In addition to avoiding being overly prescriptive on replacing "like for like," the FCC should also not condition funds on any prescriptive technology mandates. No specific technology, network configuration, or other similar mandate will be a one-size fits all solution to all network deployments. For this reason, Congress was wise to direct the FCC to implement a list of potential replacements that is technology neutral. At the same time, a recently introduced Senate bill suggests restricting any money for replacement on the condition that the relevant carrier must develop and submit a plan certifying that it will migrate to an open solution within seven years. While the intent of that bill is to encourage U.S. based 5G entrepreneurship, its timing brings with it some practical challenges.

The reality is that fully compliant open interfaces as specified by the ORAN Alliance, the most relevant in this context, have not been deployed anywhere in the world yet. These are new grounds for the industry. In fact, it is uncertain whether the most critical interface specified by ORAN will be deployed widely, as alternatives are already being proposed by several contributing, significant members. Likewise, virtualization, an orthogonal technology to ORAN, that can also facilitate open systems, has only been deployed by one carrier globally in a 5G Radio Access Network. In short, there is limited maturity in both ORAN and Radio Access Network virtualization. For this reason, Nokia believes that putting these burdens on rural carriers, the least capable of being early adopters, would be unreasonable and should not be a pre-requisite for Federal funding to replace their existing equipment, at this time.

The Challenging Marketplace for 5G

Speculation about "the Race to 5G" and anxiety about which countries will lead and which vendors will prevail has been a staple of public commentary for the last couple of years. Much of that commentary and anxiety has suggested that non-Chinese vendors are not capable of matching the breadth or quality of products offered by Chinese suppliers and, as a result, would not succeed. While that argument is incorrect, there are areas of concern that need to be addressed.

The U.S. was the first country in the world to launch 5G in the fourth quarter of 2018, followed by more significant launches in April of 2019. The U.S. was also the first country in the world to launch 5G based on mmWave. The first to launch 5G on low band frequencies, nationwide. The first to deploy a virtualized solution. And the U.S. will also be the first globally to launch what is called a Standalone 5G core network and the first to launch a technology called Dynamic Spectrum Sharing or DSS, allowing 5G and 4G to be deployed on the same spectrum. These firsts have and are being done by Nokia, Ericsson and Samsung. So, it is factually incorrect to say non-Chinese vendors are incapable of leading in 5G.

That does not, however, mean that the marketplace is without challenges. Policymakers should note that the pressure on many global wireless operators to reduce capital and operations costs, if very high, even as they deploy 5G networks, is very high. Against this backdrop, government programs including export credit agencies play a very significant role in coloring the attractiveness of supplier pricing. China has made aggressive use of its development bank and other programs to support its indigenous suppliers. Other nations have been far more reserved. For example, the U.S. Export Import Bank has not focused on telecommunications infrastructure projects in many years.

The payment terms being offered by Chinese suppliers suggest the underlying financing mechanisms, while legal, are neither consistent with commercial norms, nor available to competitors from commercial banks. We believe this is an approach that is common across many markets now based on requests from some of our customers to match these lengthy, low-interest payment terms. We raise these lawful finance mechanisms to ensure that Congress and the Administration know that they have tools available today to make a considerable difference in the competitive balance in the coming years through existing institutions.

The U.S. Export Import Bank and the recently renamed International Development Finance Corporation could potentially provide billions of dollars of grants, direct loans, loan guarantees, and insurance to exporters of 5G technology with its origins in the U.S, including to Nokia. Fortunately, there is movement in this direction now that reauthorization has been completed and the Administration appears to support moving forward as well. I encourage Congress to express its support for using these important programs to support trusted suppliers and to help them compete on a more level playing field internationally.

An additional challenge is that the Chinese telecommunications market is massive and dominated by domestic suppliers that collectively provide more than 70 percent of the equipment for LTE networks, a figure that is likely to go higher in 5G. That places Chinese suppliers in a position whereby they can spend massively on R&D and use that depth in foreign markets. Policymakers here in the U.S. and other nations that want to ensure a diversity of suppliers should work to coordinate their own R&D support programs might be utilized and coordinated to support a level playing field. To date, much of the R&D spending in the U.S. has been in support of foundational research through funding of incubators via the National Spectrum Consortium and U.S. Connect. The recent Senate Intelligence Committee bill authorizing significant funding for research on network virtualization is an additional opportunity to provide essential research support. These are well designed efforts showing the potential for promising returns, but they are ultimately insufficient in scope and resource level. The missing components are support for further 5G product development, 6G foundational research, and support generally for creating new manufacturing and industrial base development activities in the U.S.

5G Security Planning and Nokia's Supply Chain Practices and Policies

I would like to turn now to the topic of 5G readiness and security. It has become widely understood that 5G will enable advanced, new use cases supporting critical services such as autonomous driving, factory automation, connected healthcare and others. These, combined with an architectural approach that includes virtualization and distribution, increases the inherent risk and potential damage caused by bad actors on 5G networks. Putting it another way, as 5G expands beyond smartphone users, and IoT devices start to play a larger role, the network attack surface increases. This has given rise to concerns about whether 5G is "ready" from a security perspective. We believe it is for several reasons.

First, learnings from LTE networks and the vulnerabilities encountered in them have been addressed by improved security mechanisms in 5G standards as specified by 3GPP. For example, in 4G networks, the identify of users is often transferred "clear" across the air interface. This has allowed "IMSI hackers" to capture user identities and use them maliciously. This has been corrected in 5G through encryption of user identities. At this level, 5G is a significantly more secure system. Second, in addition to improving interface level security, 5G also introduced network wide security through the concept of secure, virtual "slices" across networks that cannot be breached by users in other slices. Visualize a government "slice" across a public network, that is protected and unreachable by users in a public smartphone slice.

However, even with these improvements, the reality is that bad actors could still infiltrate a 5G network. In other words, you still must trust suppliers to not act maliciously even with improved, standardized approaches to security. In that regard, Nokia does not support the view that either product or geographic isolation are effective. A breach in one part of a network could extend to other parts of the network. For this reason, Nokia believes the final and most important element of a secure system, comes from the governance models, ethical behavior and product development processes that suppliers demonstrate and apply. And here I would like to provide Nokia as an example.

One of the reasons for Nokia being on Ethisphere's ethical honoree list comes from internal governance that mandates both corporate and personal ethical behavior. Training in ethics and reporting of unethical behavior is mandatory for all employees and is a prerequisite for employment with zero tolerance.

At the product level, Nokia systemically ensures that the products we deliver are secure through a Design For Security (DfSec) governance model that involves security testing of all product releases and continuous monitoring of all software components used in our products for vulnerabilities. Product teams have structured processes and enforced timelines for how any uncovered vulnerabilities must be handled and communicated to affected customers. To ensure our own products are secure during this process involves strict guidelines related to coding, hardening, testing, and updates. Processes we expect of 3rd party suppliers as well. Transparency and a governance model for corrective action are part of how we deliver products.

Finally, Nokia monitors a number of networks through a Threat Intelligence Lab. Results from that lab allow us to understand and deliver updates to customers to proactively prevent wider issues.

I hope that this information provides a meaningful basis for U.S. consideration about future supply chain activities. It is critically important that policymakers understand what is actually done today to ensure component security, product security and post-sale security support before prescribing new regimes for testing or certification that could impose costs on your trusted suppliers without necessarily providing a security dividend. And that is where a supply chain security strategy really should begin, careful assessment of known risks and current industry practices. Actions the U.S. might consider should draw from areas only where gaps are perceived. In helping industry to be a constructive partner in this process, Nokia recommends the following:

- Identify best practices in design for security, supply chain validation and post-sale support and encourage the adoption of those practices;
- Rather than focus on countries of origin for component sourcing or manufacturing, specify the components or activities that give rise to the risk of exploitation or manipulation. Not all components and products create risk. Narrowing the focus to specific components or products with risk will assist suppliers in making critical and cooperative decisions with governments about supply chain activities.

Thank you again Chairman Thune, Ranking member Cantwell and members of the Committee for the opportunity to testify here today.

The CHAIRMAN. Thank you, sir.

And Dr. Lewis.

STATEMENT OF DR. JAMES A. LEWIS, SENIOR VICE PRESIDENT AND DIRECTOR, TECHNOLOGY POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS)

Dr. LEWIS. Thank you, Mr. Chairman.

Mr. Chairman, Ranking Member Cantwell, thank you for the opportunity to testify.

We hear that 5G is a race the U.S. cannot lose but if it is a race, we are not losing. Let's review some key issues.

The U.S. has not been rebuffed in Europe. The U.K. decision is best seen as a partial ban. Europeans agree on the risk of using Huawei and the EU calls China a systemic rival.

Where there is disagreement is over how to manage risk. Germany has a dilemma. If it bans Huawei, China has threatened to retaliate against German exports and China is Germany's largest market. German car companies have allegedly asked Chancellor Merkel not to ban Huawei and Germany is tempted to copy the U.K. partial ban.

Those who advocate a partial ban argue that if properly implemented, it makes the risk of using Huawei equipment acceptable. A full ban is best, but if countries decide against it, the U.S. will need to help make partial bans effective.

Spectrum is not an obstacle. Telecommunications companies say that the spectrum allocation process could be faster and cheaper, but spectrum decisions have not put the U.S. at a disadvantage.

The key issue, as you know, is finding ways to share spectrum now held by DoD. Standards are a battleground but in 5G, it is a battle where the U.S. is doing well. This could change if U.S. export controls handicap our companies. This is a self-inflicted wound we must avoid.

Telecoms' technology is changing. The telecom supply chain will depend on technologies where the U.S. leads, like semiconductors. Blocking exports of semiconductor manufacturing equipment is the best way to preserve this lead.

Huawei does not sell the best 5G equipment. A review by a European intelligence agency found that Huawei was the most vulnerable to exploitation. Nokia and Ericsson offer better and more secure 5G technology.

U.S. companies are strong in the markets that 5G will enable. We face tough competitors but the chief risk to this U.S. strength in 5G innovation will be badly designed privacy rules.

The doomsday argument is that because of the slowness in 5G deployment and the lack of spectrum, American entrepreneurs will not be able to take advantage of 5G, but the U.S. is not slow in 5G deployment and spectrum allocation is not an issue.

5G is a symptom of a larger problem. We face a powerful opponent who is using espionage and predatory economic practices, including exploiting American patents to gain advantage. 5G is part of this contest.

Our strategy is strength in America's technology base, work with allies, and hold China accountable, and many of the bills introduced recently by this Committee and others move us in that direction.

To summarize, I believe America's 5G problem is over-stated. If we take the right steps, we can win this race. The larger issue is how to deal with an increasingly hostile China.

Thank you, and I look forward to your questions.

[The prepared statement of Dr. Lewis follows:]

PREPARED STATEMENT OF DR. JAMES A. LEWIS, SENIOR VICE PRESIDENT AND DIRECTOR, TECHNOLOGY POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS)

Mr. Chairman, Ranking Member Cantwell, distinguished members of the Committee, thank you for the opportunity to testify. The fifth generation of telecommunications network technology is an important development and I hope my testimony can dispel some of the myths and offer a path forward for American prosperity and security.

We often hear that 5G is a race the U.S. cannot lose. It sounds dramatic, but I am not sure what it means. I am sure, however, that if there is a race, we are not losing. The U.S. is well positioned to take advantage of 5G technology, just as it did with 4G. The difference this time is we have real competition, a competitor who is well resourced, with a strong technology workforce, and a long record of unscrupulous behavior. We face a dynamic competitor in China, and there are things the U.S. can do to strengthen both its security and its technological leadership. Congress can play an important role in this.

The 5G issue has become politicized and this shapes reporting in unhelpful ways. Let's dispel some of the myths. First, the U.S. has not been rebuffed in Europe. In speaking to colleagues in the UK and Europe, there is broad agreement with the U.S. on the risks of using Huawei. The UK action is best seen as a partial ban on Huawei. The UK has blocked Huawei from two thirds of their network and from being used in sensitive areas around government and military installations. They and other European countries are committed to maintaining supplier diversity and avoiding Huawei dominance. The U.S. needs to find ways to benefit from these shared concerns to develop secure telecommunications networks.

Where there is disagreement is in how to manage risk. The U.S., Japan and Australia have banned Huawei technology in their networks. This is the only way to eliminate risk entirely. Those who advocate a partial ban argue that if properly implemented, it makes the risk of using Huawei manageable. Some European countries will copy the UK's decision. This provides the U.S. an opportunity to work with our allies to ensure that a partial ban reduces risk and there could be real advantages for the security of telecom networks and cybersecurity. The recently issued European Union 5G Toolbox provides a framework to guide policy in a way that, if implemented fully, would reduce China's use of telecom infrastructure for espionage and influence.

A full ban is the best outcome for security. It is not, in the judgment of some of our allies, the best outcome for their economies. Germany, for example, faces a dilemma. If it bans Huawei, the Chinese have explicitly threatened to retaliate again German auto exports, and China is Germany's largest market—China is playing hardball. German car companies have reportedly asked Chancellor Merkel not to ban Huawei. However, if Germany uses Huawei, China's intent is to use espionage to hollow out the German industry, and in particular the auto industry. If countries ultimately choose a partial ban, we will need to work with them to ensure that it is well implemented.

There is a larger debate over whether banning Huawei from the "core" of telecom networks and confining them to the "edge," such as the Radio Access Network (such as the cell tower that connects your phone to the network) will actually work. U.S. and Australian agencies say no, the UK and others (including some American tech companies) say yes. Frankly, the issue is moot. The UK has chosen a partial ban, others will follow them. It would be best for security if countries adopted a full ban, but if they do not, the U.S. needs to help make the partial ban as effective as possible. There is concern about how Germany may implement a partial ban, but the way to persuade it and others to cooperate with the U.S. is not by using heavy-handed threats to cut intelligence sharing. All Europeans say this doesn't help our case and if we use a more deft diplomacy that focuses on winning European cooperation in the battle against Chinese espionage, we are more likely to be effective—the Europeans are already aware of the problems of doing business with China, having declared that China is a "Systemic Rival."

The root of the 5G problem is Chinese espionage and Chinese predatory economic practices. Our European and Asian partners have realized the extent of the Chinese espionage campaign against them. Countries near China are eager to cooperate, but there is an ambivalence in Europe. China is not a military threat to them and there is a reluctance to admit that the China market that Europe depends on comes with real economic risk. Europeans say they want "technological sovereignty," to be free of both China and the U.S., and they cite Snowden in an effort to show moral equivalence between the U.S. and China. Spying, illicit subsidies, and predatory pricing helped Huawei to drive western telecom manufactures from the market and other sectors of the European economy, such as aerospace and automobiles, are now at risk. Our task is to persuade European allies that it is better if the democracies stand together.

Spectrum for 5G is not an issue. The FCC and NTIA have done a god job at supporting 5G deployment. In talking to major telecommunications suppliers, they say it would be nice if the spectrum allocation process was faster and less expensive, but most say that it is working well to meet their needs for 5G. Spectrum decisions have not put the U.S. at a competitive disadvantage. The U.S. has one of the most flexible regulatory frameworks that permits operators to migrate to another technology in a wide range of bands. The United States is one of the first deploying in high bands but we are also seeing deployment in other bands. 5G will be deployed in the low, medium and high bands in the United States. U.S. spectrum allocations have created demand for tech companies to develop solutions that will allowed for 5G rapid deployment.

The complaint that the U.S. has mismanaged 5G spectrum allocation has led to a variety of strange proposals, such as a Federally-operated 5G network or a Federally-anointed spectrum monopoly. All of these are silly and one way to explain this is that government monopolies were a good economic policy in the 15th century but have not worked as well since then. The best 5G policies rely on market forces. If there is an issue in spectrum allocation, it is one the Committee if very familiar with, and that is the process for deciding when the U.S. Department of Defense should retain spectrum or when it should be reallocated for economic purposes. NTIA has done a good job of balancing security and economics, but in the new international competitions, emphasis on economic benefit might better serve U.S. national interests.

Standards are a battleground, but in 5G it is a battle where the U.S. is holding its own and retains the lead. This is not an easy fight. China is politicizing the standards process, flooding meeting with its experts, and is already leading in some bodies like the International Telephony Union (ITU). This is not the case for 3GPP, the standards body responsible for 5G. Its rules block efforts by one government to seize control and frankly, Chinese technology is in many cases inferior, making people reluctant to use it as a standard. Interviews with leading American 5G companies show that the 3GPP standards process is still led by western companies, not China.

One crucial element for maintaining this advantage is to not see expanded export controls inadvertently damage the ability of American companies to participate in standards discussions. The U.S. Department of Commerce rules have created uncertainty. It is not good for U.S. companies to be sidelined in standards discussions by our own rules while Chinese companies are not.

Huawei is not the only supplier of 5G technology, nor is it the best equipment available. In fact a review by a European intelligence agency found Huawei was the most vulnerable to intelligence exploitation because of engineering and software problems. Huawei has undeniable strengths, and of them is its public relations department. Which has had considerable success in persuading people of the necessity of buying from Huawei as it is the "only" supplier of 5G technology which they must buy if they are not to "fall behind." Nokia and Ericsson offer 5G technology that is better and more secure, and Samsung is also establishing a presence in the 5G market.

The discussion of 5G has been shaped by the precedent of the internet, a technology that has reshaped corporate fortunes and national economies. People assume that 5G's economic effect will be the same, but this should come with a precautionary note. The Internet was created in the 1970s, commercialized in the 1990s, and began to rapidly reshape markets in the first decade of this century. Change is not instantaneous and the idea of falling behind unless you immediately install Huawei completely misrepresents the economics of digital economies.

5G (and Wi-Fi) will enable connections between sensors, the data they create, and powerful Internet computing resources. Innovators can take advantage of this connection to create new services and applications. These will be new enterprise and industrial applications such as smart seaports, hospitals, or factories. Self-driving cars are part of this and 5G will speed their use.

5G could be the start of another round of innovation and growth similar to what we saw with the arrival of the internet, but for this to happen, 5G must be accompanied by "complementary investments." These include the invention of new products and services that make use of 5G networks, and the development of new business models and processes that can profit from 5G. The U.S. is strong here, but so is China. The need for complementary investments and innovations put the "race" metaphor in context, because what companies and countries do with 5G is more important than how quickly they deploy or how "much" 5G they have.

The doomsday argument is that because of slowness in American 5G deployment and the allocation of the wrong spectrum frequencies, U.S. inventors will not be able to come up with innovations that will take advantage of 5G. But the U.S. is not slow in 5G deployment and the spectrum issue is not a significant obstacle.

China does not lead in 5G. China will have more 5G phones or cell towers simply because it has more people, but this is the wrong thing to measure. American and Chinese deployments are roughly equivalent, with 57 cities in China that have 5G as opposed to 50 in the U.S. The key metrics are revenue and market share from the ability to use 5G to create economic growth.

Companies will use 5G services to be more efficient and innovative, and innovators will create new services and products that 5G can enable, but what ultimately counts is how people use 5G to make money.

One way to make money from 5G is to sell the technologies that enable it. This is where much of the public attention has focused because of the security risks. There are five companies that sell telecom network technologies—Ericsson, Huawei, Nokia, ZTE, and Samsung—but they sit atop multinational supply chains that are largely American, Japanese, and Chinese companies that make hardware and software components used by the five major suppliers.

Another way to make money is to sell 5G services—this is what telecom companies will do. The most "disruptive" way to make money, and the way that probably offers the best outcomes for economic growth, is to create applications (apps) that take advantage of 5G. Your smartphone is in effect a tiny computer. The change in how people use the internet, from desktops to smartphones and apps, helped American companies define the mobile Internet and create the "app economy" that rapidly grew to be worth billions of dollars. 5G industrializes the app economy and expands it beyond games and other consumer programs, and this is where the opportunities for economic growth will appear. 5G will move the app economy from consumer applications (like Angry Birds) to industrial and enterprise applications.

It is true that Europe and China announced they intend to dominate 5G the way the U.S. dominates 4G, and American companies face new competition, but success depends on making products and offering services that appeal to the market. The most important market segment for 5G will be enterprise applications that allow companies to operate more efficiently and productively. Examples of these enterprise apps would include supply chain management systems, customer relationship management systems, and knowledge management systems. So far, the "killer app" for 5G has not been created, but U.S. companies are strong in these markets. It is not credible to expect the nimble, well-resourced, and entrepreneurial U.S. tech sector being squeezed out of a profitable market.

The policies that promote success in each of these areas are different. For technology producers, the focus on competition is over 5G's intellectual property, standards, and patents. Policy should encourage and support R&D, protect intellectual property, and ensure a level playing field in international standards and trade.

Each competitor has different plans for 5G. Germany intends to use 5G for industrial applications, part of its "Industry 4.0" plan, and its strong manufacturing sector may give it an advantage. 5G will play a central role in the development of smart and self-driving cars, and all countries with an automotive industry will compete in this. China already has valuable consumer apps (like WeChat), a strong developer base, and will also pursue industrial and enterprise applications. China had an advantage in developing apps for the Internet of things since its companies are the source of many of these products. But Chinese companies also face trust issues, since any Chinese-made device that connects to the Internet could be exploited by Chinese intelligence agencies.

Telecom technology used to be somewhat static, changing slowly. It relied on specialized hardware, each generation providing incremental improvements over the prior in speed and reliability. New technologies like cloud computing were layered on top of established protocols and equipment. This is now changing. Telecommunications technology is now going through a transition similar to the effect of the commercial Internet on computing three decades ago. This has major implications for security and business.

The move to an open, modular approach to telecom will change supply chain dynamics in ways that favor the U.S. (and Japan). The supply chain for telecom will depend on semiconductors, chipsets, and specialized software (including "open source" software), all areas where the U.S. has a substantial lead over China—in some cases there are no Chinese competitors. Estimates of how long this telecom transformation will take range from three years to a decade. The shift puts Huawei at a disadvantage. China will of course invest to catch up (accompanied by increased espionage), but money alone won't remedy China's lag in software and semiconductors.

The most visible aspect of this change is Open Radio Access Network Alliance, an industry group developing architectures and software that will enable virtualized networks (*e.g.,* those based on software rather than hardware), commodity computers, and standardized interface.

The companies that make the modular components for new telecom technologies included both familiar names and new startups. Qualcomm, Intel and Samsung make chips. Microsoft (which has a huge 5G lab) writes operating system software. Cisco, Sienna, Xilinx, Nokia, Fujitsu, and NEC make other essential components, as do a number of new companies, such as Altiostar.

These are all American, Japanese or Korean companies. In contrast, Huawei's strength in the new technologies is in RAN cell towers.

It is much easier to tell a story of gloom and peril, but it's not a good guide for law or policy. There are, however, steps we need as part of a comprehensive approach to 5G. The three most difficult challenges are rebuilding the sources of American technology leadership, effectively partnering with allies, and resisting China's efforts to use espionage and predatory trade practices to attain dominance. These are not unique to 5G and it is important to see 5G as only a part of a larger technological competition.

Some recommendations are things the Committee has heard many times, such as rebuilding the American tech workforce through investments in college education and spending more on R&D for the "hard sciences." It's worth noting that these steps would help with competing with China in the standards battle by expanding the tech and engineering workforce needed for the standards process.

An implementable suggestion is to restore the STEM scholarship programs established by the Eisenhower administration in reaction to our last technological security threat in the 1950s. This means paying students to study engineering, math, sciences, coding, and languages. The Chinese are not reluctant to spend money to build their tech workforce and is this is one of their greatest advantages over us.

The U.S. can safeguard the standard process not only by increasing the number of American participants, but by working with European and Japanese partners to ensure that standards bodies remain open and equitable, and with governance structure that remains able to resist efforts to politicize or capture them.

A crucial element of maintaining a U.S. presence in standard bodies is to make clear that export control regulations do not prevent U.S. companies from participating in international standards discussions. The Commerce Department needs to immediately clarify that standards participation remains exempt from export regulations. This is a self-inflicted wound that the U.S. must avoid.

R&D funding for the development of industrial apps and the Internet of things is important. While market forces will drive some of this, we can accelerate 5G deployment and the benefits to the U.S. economy by supporting additional research. DARPA has a program on 5G security. NSF and NIST have small programs in these areas, but they are dwarfed by what China spends. We cannot expect to maintain technological leadership when we are routinely outspent. An easy suggestion would be to double the funding now allocated to 5G and cybersecurity.

There has been some discussion of whether to help Nokia and Ericsson, the two European 5G equipment manufacturers, ranging from support for R&D to outright purchases of the companies. An initial and relatively uncontroversial step would be to find mechanisms to support R&D by these companies. No option is off the table and there is perennial talk that one of the companies will be bought or merged. In the next decade, Nokia and Ericsson face the challenge of adjusting their business models to accommodate changes in telecommunications, since the proprietary "stack" that they and Huawei make will be overtaken by technological change. In the near term, it is in our interest to ensure that they continue to operate profitably and can compete on equitable terms with Huawei. One approach would be to instruct DOD to develop Cooperative Research and Development Agreements (CRADA) with both companies, to fund their R&D.

Some recommendations may seem at first glance unrelated to 5G. 5G depends on semiconductors, and the U.S. is the leading source of supply. The Chinese government does not like this and intends to develop its own semiconductor industry to replace American firms both in China and in the global market. But to make chips, China needs to buy semiconductor manufacturing equipment (SME) which it cannot produce itself. The major sources of this SME are the U.S. and Japan, along with one or two European companies. One way to limit China's role in 5G is to limit exports of SME. Some of our allies have proposed augmenting existing controls to do this. We should develop a new SME export control regime with our Japanese and European partners, and Congress can help the Administration focus on this by mandating it, with timelines.

I hesitate to make recommendations on spectrum, since the process is working well enough and since any effort at reform raises powerful antibodies to block change. Congressional interest in seeing the allocation process further streamlined and in reducing the ability of a single agency to block reallocation would be helpful for the mobile network world we have entered.

We face a difficult challenge of managing the transition from the older model of telecommunications technology to the new, internet-based approach. Some say this transition will be here in three years, others say a decade, but the goal for now is to keep the two European suppliers viable and technologically sound. To some extent this can be left to the market, the customers of these companies will encourage them to evolve, but the U.S. can assist by emphasizing this in decisions with the governments of Sweden and Finland.

Whether or not other nations follow the UK precedent of a partial ban, we and our security problem will continue to confront the challenge of how to communicate securely over networks with untrustworthy components. Finding a way to do this, and to help those countries that choose a partial ban make it as effective as possible, is a central strategic goal for the U.S. The Prague Principles for secure telecommunications networks produced last year are a starting point for this, and the U.S. can strengthen these principles at the upcoming second meeting, by aligning them with measure criteria for security. It is not enough to say that we should avoid a telecom "monoculture." There must be an explicit commitment to buy from multiple venders and to give preference to suppliers from democracies even if the price is higher.

Huawei is a symptom of a larger problem and 5G is a symptom of larger fears. We face, for the first time in decades, a powerful, unscrupulous, well-resourced opponent who has publicly declared their intent to displace us. We are not ready for this fight and do not have a strategy to respond to this challenge. It is likely that for some time we will be unable to develop such a strategy. This is not a reflection on American politics, messy as it can be. It reflects that we are in a different kind of competition. Increasing the defense budget will not help the U.S. win. This is a competition over markets and technology, things with which the foreign policy and defense establishment are still unfamiliar. Strategies that traverse the intersection of economics and security will not at first be easy for the U.S. to construct.

China has strengths—a determined Leninist leadership willing to spend on strategic goals (and even though the U.S. is twice as rich as China, we are being outspent), an immense domestic market, and a plan to shield this market from competition while using it as a base to dominate a range of industries, assisted by predatory trade practices and a massive economic espionage campaign. China has weaknesses as well—the heavy economic costs of a repressive regime, the inefficiencies of state capitalism, clumsy diplomacy and, above all, a fear by the Party leaders of their own people. China is not our technological peer but they are making immense efforts to change this.

The U.S. needs to act in response. We have seen some efforts in the last few years, but more needs to be done, including a revitalized science and technology base and a coordinated approach with our allies on how to respond to China's espionage, unfair trade practices, and efforts to reshape global rules to better accommodate authoritarianism.

To summarize; the problems often attributed to 5G in the U.S. are often overstated or wrong; there are things we can do to speed up deployment and reduce risk, but the larger issue is to how to deal with an increasingly hostile China in a new kind of non-military competition. Thank you for the opportunity to testify and I look forward to your questions.

The CHAIRMAN. Well, thank you. Thank you very, very much.

Let me just make sure. Dr. Lewis, is your testimony the official position of CSIS?

Dr. LEWIS. CSIS doesn't take official positions because we're either a nonpartisan or bipartisan, I forget which one it is, but we're——

[Laughter.]

The CHAIRMAN. Well, I always thought you were bipartisan.

Dr. LEWIS. Well, and I always thought because I was a career officer I was nonpartisan, but in any case, it's the individual scholar's, not the entity itself.

The CHAIRMAN. OK. So you don't think the sky's falling and we're doing just fine in the race. Everybody on the panel agree with that? Anybody like to comment or respond? Mr. Murphy?

Mr. MURPHY. As I indicated, I mean, factually, the U.S. has led in a number, first, for 5G, with the first deployments in the fourth quarter of 2018 followed by more commercial systems in April 2019, the first millimeter wave, the first to deploy low-band spectrum nationwide with T-Mobile, the first with virtual network solutions in Verizon.

So it is factually incorrect to say that non-Chinese vendors are leading and there's a disadvantage [Off microphone comments]

The CHAIRMAN. We may have a bit of a bug or two with our public address system.

Let me put it this way and be careful how I choose my words. Many of us are concerned that we may lack in affordable and viable alternative for end-to-end communications equipment to compete effectively in the global market.

What can the U.S. do to strengthen its supply chain security requirement and is there in fact, Mr. Berry, we'll start with you, a viable alternative to Huawei and ZTE equipment available in the market? Mr. Berry and anyone else?

Mr. BERRY. Thank you, Mr. Chairman. Well, first, what you did in the Secure Trusted Act, you know, was a monumental movement forward because you identified the need for the FCC to create a list of suggested replacement, *i.e.,* providers, trusted vendors, that are available to everyone.

Most of the smaller carriers don't have the technology, not the technology but the employment, you know, gravitas to do all the research to identify what is a trusted provider. So that, I think, is going to be a huge improvement on the supply chain.

I think it will also lead to some of our members, and we not only have Nokia and Ericsson sitting at the table but some of the new entrants, like Mavenir and Parallel and others that are U.S.-based, looking for new technologies, and I think that requirement that the Federal Government identifies secured communication providers, equipment providers will help us move forward quickly on alternatives.

I agree, I think we need to be ever vigilant on that, but I don't think it's an impossible task, and I think the bill that you just passed has done two things: provide information on a continuous basis and with creating a list, you have essentially directed the Federal Government to be involved.

I don't think it's a one-shot pony. I think they're going to have to be involved every day providing good guidance to carriers throughout the United States.

The CHAIRMAN. Ms. Keddy.

Ms. KEDDY. Thank you.

The CHAIRMAN. If you would move that microphone? It's pretty long for a petite person.

Ms. KEDDY. Thank you. So I think the U.S. has been involved and I believe that the focus should be on innovation.

If you look at 4G, we had many companies that didn't exist before, like ride-sharing companies, Airbnb and all. So the faster we have widespread roll-outs across the Nation and sort of just the first, the better off we are, and I thank you for many of the acts, including the Telecommunications Act, where R&D is invested and it's a starting point.

We believe that the government can do more to help new entrants and while maintaining existing incumbents, so that we have a diverse supply chain. Virtualization is a key and the faster we have widespread deployments, including with spectrum and all, the better off we are because the innovation about 5G is really focused on other industries, like the power that we give to consumers in 4G. We would like to bring it to other industries, like aviation, agriculture, and other economies, and centers also are important.

Thank you.

The CHAIRMAN. Mr. Boswell, would you like to weigh in briefly?

Mr. BOSWELL. Thank you, Chairman Wicker. Yes, I think Ericsson's been a leader in secure 5G not only in the U.S. but worldwide in rolling out networks and the reason is we've been planning for this for a decade. We've been building the standards and getting radios ready for what is coming right now for a long time.

Going back to 2015, Ericsson radios that are in the field, of which we have several hundred thousand, are ready for 5G today with software upgradability. So that kind of foresight and planning has allowed us to actually kind of be ready to go full steam ahead on that race to 5G, given that other kind of accelerators line up, as well, such as spectrum and small cell siting and making sure our workforce is skilled and ready, as well.

The CHAIRMAN. Thank you.

Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman, and before I get into questioning, I would wonder if we could—I'm a little uncomfortable today not seeing a press table. I know that we have press in the room, and they look like a resilient bunch of people who are just writing away no matter what.

But I would feel more comfortable if we asked Senator Blunt where the press table is supposed to be in the room. Then, we could accommodate both the press having a place to write and feel comfortable here and having some audience participation. So I'm sure he's working on it or something. Well, let's ask him when he comes.

OK. To the 5G question, Ms. Keddy, I hate to say decades ago I was involved in trying to fight a past the Democratic Administration on the Clipper chip. I felt that was a bad idea, too. The notion that in the 1990s we thought the government should have a backdoor to ease our concerns about great encryption capability, and I kept thinking instead of saying Intel on inside, you were going to be saying U.S. Government inside.

So it didn't work when we thought about it, and it shouldn't work today. And since you're a global company, and Dr. Lewis, your comments about we're not really that far behind, I don't know why we can't get parts of Asia, parts of Europe in a more unified voice around communications equipment that any company that has a government that is demanding access to that technology as a backdoor is just unacceptable.

We need to just build this international alliance to just say it's just unacceptable. You want to be a mature economy. We're not against your companies. We're against the fact that you demand a government backdoor to them. That's what we're against. So I don't know why we can't build that international coalition and communicate.

So, Dr. Lewis, Ms. Keddy, either one of you?

Ms. KEDDY. We look at information security in two ways, right, and so security has information security and supply chain security and we look at how do we have security constructs in both ways.

As far as to your question on backdoors, I think that the government knows a lot more details than us and so we look forward to working with the government to support the requests that is provided versus being able to mandate it as a private company.

Senator CANTWELL. Dr. Lewis.

Dr. LEWIS. Thank you, Senator. First, the U.S. could benefit by making it clear to other countries that there are alternatives to Huawei.

When I travel to Asia and to parts of Europe, I hear this. Well, Huawei's the only place we can buy from. That's complete nonsense, but we have to do a better case of getting the alternatives out there.

Second, as I think some of my fellow panelists have mentioned, U.S. support for exports would be helpful. That would help us not match the Chinese but at least reduce what we used to call the Huawei premiums. So export support is a crucial part.

Finally, we are starting to build an international coalition. It's been a little bumpy. It's not NATO. It's not ASIAN, but it has members of both, and we could perhaps be a little smoother in our approach sometimes. It doesn't help to threaten people, but I see an international coalition emerging.

Senator CANTWELL. Ms. Keddy, did you want to add something to that?

Ms. KEDDY. If I can add to Dr. Lewis' point on ensuring like a standard base but diverse supply chain that gives more choices, that will also help the options but in the case of these events do happen, I wanted to emphasize the notion of technology problems to technology solutions, so we can prevent and detect all of these.

Senator CANTWELL. Well, I think, Mr. Murphy, you're the CTO, right? So you're probably our most technical person here. I mean, Ms. Keddy, you probably have, but this is—look, we should just like—you know, there are lots of examples of where even if you had to put, you know, the crown jewels into some sort of repository or something just to get cooperation and interoperability, you could do that, but this notion that we're not fighting this on a big broad principle is just crazy.

Like you've got to fight the principle. The principle is we shouldn't live in a world today where any government has a backdoor to technology. Like that's just not the way we want to deploy, and that has to be consistent. It might be 5G now but it will be something else later. And the more we communicate that—the reason why I bring up the Clipper chip is we made the same—well, we almost made the same mistake.

You know, the U.S. Government started saying, oh, my gosh, don't want that level of encryption. I got to have a backdoor. We're like no, we're not having a U.S. backdoor.

So I think this is the conversation that now needs to take place in Asia and hopefully because it has many ramifications for cloud and cloud services. That's one of the things they've been demanding. Oh, you want to do cloud business in Asia? This is what you got to do. Give us access. No, we're not going to give them access to that.

So this is a global effort we need to communicate about.

So thank you. I'm sorry. I think——

Senator GARDNER. Thank you, Senator Cantwell.

Senator Fischer is next.

STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Senator Gardner. Thank you, Senator Cantwell.

I am glad that the Secure and Trusted Communications Networks Act made it on to the President's desk last week, and I was proud to be a co-sponsor of that companion bill in the Senate last year.

This legislation is critical to create a stable and secure foundation for America's communications networks. However, it will also set the stage for carriers' ability to meet timelines established in the legislation and how applicants can request reimbursement.

Mr. Berry, are there still small providers who haven't been able to secure commitments from trusted vendors to assure that they can deliver the quantity of equipment needed for the networks within those timelines?

Mr. BERRY. Thanks for the questions, Senator. Yes, that is a difficult task for many small carriers.

What we're seeing with this legislation, especially when you kick-started the concept of you may actually be able to replace that covered technology with new technology, our carriers are already out there getting vendors and getting equipment manufacturers to give us quotes and to give them estimates of what it's going to take.

As a matter of fact, several on this panel have already been involved with detailed conversations with the small carriers. Our intent is not to let any moss grow on this stone. We want to make sure that we're out there trying to find the solution ASAP and, yes, new technologies could in fact create new security opportunities, but there is a time lag. There is a flexibility, a need for flexibility.

Some of the technology may not be ready to deploy today. It may be ready in five-six-eight months, a year and a half. So we need to measure twice and cut once and I think that maybe the small carriers, especially with this Act, will get the information they need and they're certainly ready and willing to tackle the challenge.

Senator FISCHER. You know, that information is going to require them to have information on how to apply for the funding, as well. That's going to be a big deal as we move into this for any number of reasons, not the least being security.

What are you hearing from your members? What are the questions you're hearing the most from your members who are going to have to Rip and Replace?

Mr. BERRY. I think the Number 1 issue is now that we have a goal, the goal is no covered equipment in your network. The next question is, OK, how do we prioritize that? Which elements do we take out first? Do we take out, you know, everything from the antenna back to the core? How do you do that? Do you go from a 3G to a 4G to a 5G solution?

You know, part of the problem is many of the vendors are not making the 2 or 3G technology that may be in some of these networks. So how do you get to a 4G technology when you have 3G technology but you have voice?

So it may be necessary to go to a 4G LTE VoLTE product so you replace old technology with a newer technology that actually has voice. So those things are real sort of in the weeds but they're very detail-oriented and it's what our carriers think about in terms of how do we maintain connectivity, and it is like building a separate network while you operate a network so you can transition on day one and actually you'll be able to make a call.

Senator FISCHER. Thank you. Dr. Lewis, you stated that the bans on Huawei network technology, such as in the United States, Japan, Australia, also, that that is the only way to eliminate risk entirely.

A couple weeks ago, I was in the U.K. with a handful of my colleagues and we met with the government there and obviously we expressed some concerns about their recent action, as well as the influence that that may have on actions within the EU. Those are security concerns.

The U.K. is a member of 5 Eyes. That causes us to take a step back and decide that special relationship we have with the U.K., how do we move forward on that when it comes to security measures.

Can the core really be securely isolated in a way that some of these countries are talking about in theory? The Chinese don't like this. Some countries are talking about this core and how it's going to be secure and we don't need to worry and, you know, my comeback is we have to put national security above price. How would you answer that?

Dr. LEWIS. Thank you, Senator. I think that the politics and the commercial motives that our European partners have will probably drive them to adopt a partial ban. That's not in the best interests of their security. We have the discussion of a backdoor, but they will be motivated by China's economic power.

That means for us, there are two things. First, we can help them do better at making sure the partial ban eliminates risk as much as possible. There's debate over this. I would defer to my more technologically astute colleagues, but there are some companies and some intelligence agencies that say a partial ban could be made to work in the near term.

The second issue we need to bear in mind is this is not a finished deal. The British have said, perhaps they said it to you, that their opening position is limitation of 35 percent, but they're willing to move that back as we go forward. So we need to help them to make it work.

Now we need to help them get to move in the right direction later on.

Senator FISCHER. Thank you very much. Thank you, Cory.

Senator GARDNER. Thank you, Senator Fischer.

And, Senator Rosen, in a different time zone, you may begin your questions.

STATEMENT OF HON. JACKY ROSEN, U.S. SENATOR FROM NEVADA

Senator ROSEN. Thank you. Thank you so much. Thank you all for being here and for this very important hearing.

I want to talk about how we promote the U.S. and its wireless, how we really lead in this area because we are a global leader in wireless technology and performance and innovation, and the U.S. really is at the cusp of a technological evolution.

Just as the 4G wireless industry created millions of jobs, ushering in an era of social media, the gig economy, mobile apps, 5G is going to fundamentally change the way that our industries operate.

So for the U.S. to remain a leader in this space, our response must be one of coordination and cooperation. This means working with private sector, supporting R&D and emerging technologies, coordinating with the relevant agencies and participating, I believe really importantly, in standard-setting where much of the foundational technology that makes 5G possible.

Homeland Security Chairman Ron Johnson and I actually recently introduced the bipartisan Promoting the United State Wireless Leadership Act of 2020. We want to ensure the U.S. has a seat at the table in the wireless standard-setting process because our global economic competitiveness depends on our participation in setting good standards for the next generation.

So, Dr. Lewis, I'd like your opinion on how important it is for the U.S. Government to participate in these standard-setting bodies, including the International Telecommunications Union, the 3G Generation Project, and I'd also like you to comment on what is the impact of our participation or lack thereof on technologies, including telemedicine, our connective devices, our smart grids.

Can you speak to that, please?

Dr. LEWIS. Yes, thank you, Senator. So there is a distinction between the ITU and 3GPP. One of the questions that is emerging is what the role of the U.S. should be in the ITU, which is dominated by powers that are hostile to us in many instances.

3GPP, as you've heard from some of my colleagues, we are doing better. It's essential that we maintain a strong U.S. presence there and if that includes funding for U.S. Government participation, that would be valuable.

The dilemma if we withdraw, and I'm sure my other colleagues will agree with this, the dilemma is if we withdraw is that China seeks to dominate the standards process. It seeks to politicize it and it seeks to have it pick China's technology even though that technology is not the best available.

So it's crucial for us in all the markets that 5G will enable to maintain a strong presence in the standards bodies.

Senator ROSEN. Well, that's great because it really leads to my next question about telecom equipment manufacturing.

So with the absence of a major U.S. alternative to foreign suppliers of 5G networking equipment, our wireless carriers rely on just a few companies to manufacture the next generation of 5G technology. Some U.S. companies, they sell switches and routers that reside in the innermost parts of the carrier's network but none actually build the wireless infrastructure that allows cell sites to connect with smart phones and mobile devices.

So in light of the Coronavirus that we've been dealing with in the last few weeks or months, it's clear how dependent we are on goods and commerce from other countries. A breakdown in our supply chain highlights how interconnected we are and the impact it has on our economy and our security.

So as we continue to discuss securing the 5G supply chain, can the U.S. regain a footing in 5G equipment manufacturing? What do you need from us to be able to do that or should we look to possibly 6G to regain our leadership position in the global markets? Anyone like to take that, please?

Mr. BERRY. Let me just tackle that a little. I mean, Number 1, I don't think you can get behind on your Gs ever. We can't avoid engaging in the 5G solutions, but I think some of the technologies that our companies not only here at the table but the new companies in the United States are finding to not only replace those functionalities of equipment with software solutions, *i.e.,* virtualization of the network, everywhere from the antenna back to the core and to the interface, you know, with the devices, I think we're on the cusp of finding significant opportunities for cost reduction and new competitors in the marketplace.

And so I think that that is one of the areas that we need to maybe rethink how we provide, quote unquote, equipment and functionality to the network and I think some of the specialists here that are engineers could explain that also from their perspective.

Senator ROSEN. What can we do in Congress to help facilitate us being a leader in that?

Mr. BERRY. Well, I think what you've done in the bill, the Secure and Trusted, is a huge step forward, especially for the small carriers that don't have the engineering staff to know exactly the consequences of the technology, but there are a couple bills sitting around in the House and the Senate that recognizes this as a priority and I tend to concur that we need more government inclusion and involvement with the private sector as we move forward in the standard-setting bodies and I think that would be a priority for the Nation as a whole.

Senator ROSEN. I know I've exceeded my time, but can Ms. Keddy answer?

Senator GARDNER. Please.

Senator ROSEN. Thank you.

Ms. KEDDY. I just would like to add like incentives to enable a widespread deployment across like rural and urban is very important and also virtualization and open source efforts, very vibrant new entrants that can be helped so that we have a very diverse supply chain is important. So both these things, including other telecoms acts that have R&D as a starting point, which is good, but we'd like to see it much more toward the innovations and incentives and other things for deployment.

Senator ROSEN. Thank you.

STATEMENT OF HON. CORY GARDNER, U.S. SENATOR FROM COLORADO

Senator GARDNER. Thank you, Senator Rosen, and seeing the Chairman has not returned, I'll move forward with the questions I was going to ask.

Mr. Berry, Congress has finally succeeded in passing Rip and Replace or to some Replace and Rip legislation to ensure Huawei is removed from all U.S. telecommunications networks. I've got deep concerns about Huawei and the intelligence that we've received, which functions essentially as an arm of the Chinese Central Government.

I'm thankful that your member companies are hard at work to transition their equipment and to seek new vendors and while I appreciate the dedication, I'm also hopeful that we can provide them certainty to make sure that we ensure this Rip and Replace model is not the default approach to network security in the future.

Your members and other interested parties explored these ideas at a series of rural engagement initiative events and thank you very much for hosting one in Colorado, my home state.

What more can Congress do? What more can Congress be doing to ensure better communication between the Federal Government and companies of all sizes in the telecommunications industry when it comes to long-term network security?

Mr. BERRY. Thank you, Senator, and thank you for recognizing the fact that our small carriers, as you may say, have spent a lot of time on the educational side and that's one thing, I think, that this Committee has made enormous progress on is creating the focus and creating the education about what are the security threats, what are the solutions, and I can't stress the fact that you have now directed some certainty in their lives going forward, not just for the carriers that have covered equipment in a network but if you're a small carrier, you can't afford to make the wrong decision and deploying your resources, especially when you have limited capital to invest.

And so I think the industry and the vendors in our industry, at least those that are CCA members, are stepping up to the plate and I've seen a lot of activity internally with their companies to say this is a problem, we need to be part of the solution, and I can't congratulate them more on that.

But thank you. The U.S. Chamber of Commerce joined us in those sessions. I must say that CISA was the specialist entity within the Homeland Security. We couldn't have been more pleased with the very frank discussions they shared with our members throughout all those meetings.

Senator GARDNER. Very good. Thank you, Mr. Berry.

I have a question for both Mr. Boswell and Mr. Murphy. I'll start with Mr. Boswell. Obviously the concerns about Huawei and insecurity with Huawei made clear our country's telecommunications companies and many of our allies are rapidly seeking new physical network vendors. That will largely benefit non-Chinese companies, like Ericsson.

You never mentioned Ericsson's presence in China in your testimony, but Ericsson's website talks about the company's long history in China, going back to the 1890s. In fact, it says, "Ericsson has several joint venture companies in China and has invested heavily in research and training in China which provides a competitive advantage."

You've also opened a Joint Research Institute with the Beijing Institute of Technology.

Is Chinese-sourced research incorporated into Ericsson's core network products? If so, what protections does the security team have in place, including hiring protocols, to ensure any Chinese Government-backed activities that might otherwise attempt to undermine the security of those products?

Mr. BOSWELL. Thank you, Senator. I plan to address all of those points that you make. Of course, China is a large market and we can't and don't ignore that market or any other market around the world, frankly, but we don't have production in China for the U.S. market.

In fact, back in 2018, we proactively before it was kind of a thing to be talking about, we started proactively executing a regionalization strategy for our supply chain to put manufacturing and development as close to the customer market as possible in the United States.

Senator GARDNER. Can I interrupt? Maybe we could follow up with written questions for the record.

Is Chinese-sourced research incorporated into Ericsson's core network products?

Mr. BOSWELL. So from a software standpoint, all of our software from a development standpoint actually funnels through Sweden and all of our software is scanned, verified, signed, and centrally distributed from Sweden. That gives us tight control and transparency——

Senator GARDNER. And the answer is——

Mr. BOSWELL.—in chain of custody——

Senator GARDNER. The answer is yes, you believe it's properly filtered through other vendors and systems?

Mr. BOSWELL. Actually most of the development items from a Chinese perspective would be for that Chinese market from a manufacturing standpoint. So we do manufacture things in China for the Chinese market, for example.

The majority of our R&D and development is actually in Europe and North America.

Senator GARDNER. So none of that Chinese work research that you're doing at the Beijing Institute of Technology would find its way through to products in the U.S.?

Mr. BOSWELL. I would have to follow up specifically about that, but we do maintain a tight chain of custody of our code with check-in/check-out policies to ensure that we can track back where specific things have been sourced from.

Senator GARDNER. Thank you. I'm going to quickly switch to Mr. Murphy. Nokia has nearly 50 offices across mainland China and China accounts for more than 10 percent of Nokia's sales, according to the company's website. Nokia also operates six research and development innovation hubs, three manufacturing facilities, and employs 7,000 people throughout China's footprint.

Your customers include China Mobile, China Telecom, and China Railway, among other Chinese Government entities.

How would you answer the same question that I just asked Mr. Boswell, how are you protecting the security infrastructure and what security protocols do you have in place in China to do so?

Mr. MURPHY. Thank you, Senator Gardner. So perhaps to divide that into two parts, one is manufacturing and one is R&D.

On the manufacturing side, we have a number of manufacturing plants around the world and depending on the recipient of the product, we will make the best choice for that. So, for example, in the case of the U.S., there's no equipment that is manufactured in China.

On the R&D side, as you noted, we do have research in China, but from my testimony, we apply the same standards for our Chinese employees as we do for other global employees, meaning they must sign ethical standards. It's a prerequisite of employment. Also, software goes through a design for security verification test. Vulnerabilities must be resolved and documented.

So the fact that they're physically located in China kind of is a little bit irrelevant in terms of producing a secure product.

Senator GARDNER. Thank you, Mr. Murphy. I apologize. I cutoff others. I'm a minute and 30 seconds over. So I'm going to cut myself off and I believe the next—Senator Lee, are you ready—excuse me.

Senator Thune is next. Sorry.

STATEMENT OF HON. JOHN THUNE, U.S. SENATOR FROM SOUTH DAKOTA

Senator THUNE. Thank you, Mr. Chairman, and I want to thank Chairman Wicker for holding today's hearing on a very important issue and I think we all would agree that with increased speeds and greater capacity, 5G networks are going to unleash new innovations and enable breakthroughs in a variety of sectors, from agriculture to health care.

There's a lot of promise with these new and advanced technologies, but the United States is only going to be able to deliver on those promises if we maintain the security of our communications networks, both here at home and abroad.

The decisions that we make today with our trade partners around the world are going to impact our national security and economic outcomes for years to come.

I intend to introduce legislation this week to ensure the security of our communications infrastructure as a clear negotiating objective of U.S. trade policy.

Unfair trade practices of communications equipment suppliers owned or controlled by a foreign government should not be tolerated, period.

Mr. Lewis, when we think about future trade agreements with the United Kingdom and other countries, should the security of our communications networks be at the forefront of those conversations?

Dr. LEWIS. Thank you, Senator. I think this legislation is long overdue. It is essential. Of course, it should be part of our discussions with our allies and partners and in fact in any trade agreement. So I think this is a great step forward. Thank you.

Senator THUNE. Thank you. Mr. Boswell, Mr. Murphy, 5G networks have potential to generate greater virtualization in software-defined functionalities.

Can you talk about some of the security benefits as well as the challenges that exist with these new network elements? Mr. Murphy or Mr. Boswell, either one.

Mr. BOSWELL. Sorry. Thank you, Senator. So, of course, 5G will become more virtualized and software-defined and what we mean by that is that the intelligence of the network will be located more in the cloud or in some cases closer to the edge.

So distinctions between different parts of the network may become blurred. It also actually gives us some distinct advantages as we bring in new security technologies.

Now 5G will be built on what is already a very secure 4G infrastructure, but it does bring new tools to the toolbox, so to speak. The new architectures that we will roll out and the types of technologies we will use allow us to do things like additional encryption across the network, enhanced authentication and more granular data access control for enhanced privacy protection for subscribers. I think we would all agree that's very important.

In addition, we'll have greater in-network segmentation that can provide real-time prioritized network defense and improved resilience. The availability of the network is actually that's a key cornerstone of security, as well, availability, in addition to confidentiality and integrity.

So there are new technologies that we'll see here, but ultimately it's about how we design and build in, implement, and operate those networks, as well, on top of what we see in standards.

Senator THUNE. Mr. Murphy.

Mr. MURPHY. Thank you, Senator Thune. So 5G raises the bar and lowers the bar at the same time. So it raises the bar in the sense that 3GPP specifications have resolved many of the vulnerabilities that used to exist in 4G. At the same time, we're moving toward distributed and virtualized networks, which one could argue lowers the bar, meaning they're more vulnerable.

So we still need to take action on the product side as both Mr. Boswell and myself have noted in design for security or integrity protections in the things that we produce, but at the end of the day, no matter what we do, there will always be a vulnerability that can be infiltrated and thus it always comes back to trust in the supplier themselves and this is where the behavior, the ethics, the historical performance and behavior, and the governance it puts on securing the products it produces is the most important.

Senator THUNE. Thank you. Mr. Berry, last week the Senate sent legislation by Chairman Wicker to the President's desk that would help rural telecommunications carriers remove equipment from high-risk vendors, like Huawei and ZTE, from their networks and replace it with secure telecommunications equipment.

In your testimony, you suggested the lack of availability of a properly trained workforce may impact the transition process that these smaller carriers will have to complete to remove the compromised equipment.

How will legislative efforts like the Telecommunications Skilled Workforce Act that I introduced with several of my colleagues on this Committee earlier this week help ensure the necessary workforce is in place?

Mr. BERRY. Thank you, Senator. Yes, S. 3355 is actually key to being able to stay up with the growth, the expansive growth of 5G. It would be a shame to lose the economic benefits that this new technology promises if we have a lack of trained labor force.

I think it would be a great move. We support it. There's a lot going on in the wireless world. Not only do you have the 600 megahertz that we're repurposing, that's finishing up, you've got a lot of carriers in rural America that they may only have access to their towers and to their facilities for maybe two or 3 months out of the year because of weather and other climate issues.

So having a crew that's available and the technology to deliver, you know, the labor force is critical and without it, we'll not make that transition. So thank you so very much.

Senator THUNE. All right. Thank you, Mr. Berry. My time has expired. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Thune.

Senator Lee.

STATEMENT OF HON. MIKE LEE, U.S. SENATOR FROM UTAH

Senator LEE. Thank you, Mr. Chairman. Thanks to all of you for being here.

There's what I think one could fairly characterize as a broad consensus that there are vulnerabilities in the network and that the use of Huawei equipment within the networks poses a risk of access by the Chinese Government certainly for espionage purposes and potentially for operational control purposes. Either way, this is troubling.

It does seem, however, like there's some debate among experts as to whether or to what extent this vulnerability exists in equal parts throughout the network. There are some who would draw a distinction, based on where the equipment in question is located within the network. Some have suggested that this makes a difference and that depending on where the equipment is, you might be able to manage the risk through some work-arounds.

So, Dr. Lewis, we'll start with you. Given your expertise and your experience in this area, can you clarify whether or not there is a distinction between the core and the periphery of the networks and is that a distinction that could make a difference for our security?

Dr. LEWIS. Thank you, Senator. There is a distinction. It's increasing under the development of 5G. What used to be done in the core in terms of processing can now be done in some cases at the edge, given the computing power that will reside in 5G networks.

There is a debate over how to manage this risk, and there's a third element here that might involve the use of cloud computing as the backbone for some telecommunications functions.

I think the debate is unresolved but if I had to speak, I would say if you don't want any risk, don't use Huawei. If you decide to use Huawei, you need to work hard to manage that risk, but I think it can be done.

Senator LEE. Do you know that the FCC is having this discussion internally in connection with the Rip and Replace plan?

Dr. LEWIS. I think that the FCC has come to the conclusion, the correct conclusion that the best way to reduce risk in the U.S. is to eliminate Huawei equipment.

Senator LEE. Right.

The CHAIRMAN. And Congress has come to that conclusion.

Dr. LEWIS. Thank you, sir. Thank you, Mr. Chairman.

Senator LEE. And so for similar reasons, then you would also say the same with respect to software. If you try to impose a software solution to it, it might mitigate your risk but it doesn't eliminate it. In order to eliminate it, you've got to rip it all out.

Dr. LEWIS. That's correct. You can reduce risk, but the only way to eliminate it is to remove the technology.

Senator LEE. The FCC's NPRM to establish the Rip and Replace program has been criticized, according to some, for underestimating its costs, especially when you take into account the resulting equipment options, the resulting options that will involve less equipment being available. Fewer options do tend to increase the price tag and sometimes can produce additional costs and additional delays.

Mr. Berry, is the Rip and Replace price tag of $1 billion accurate in your estimation?

Mr. BERRY. Well, Senator, thank you. It's a tough question. It's really difficult to actually know.

Right now, our carriers are going out to the vendors and asking for bids and how can you actually replace the technology. It's hard to say. I mean, a lot of it is also timing and flexibility.

For example, you mentioned availability of services, goods, and equipment, and the ability to actually, you know, build and put the new technologies in place. It's a matter of timing and the FCC, if you use a cycle of maybe a little longer than a year, I appreciate the wisdom of the Committee's legislation of a year to kick-start this but I also appreciate the fact that you have a flexible opportunity there for the FCC to give additional time, and I think with that, you can manage costs and I think we'll see as more carriers come in with, you know, verifiable cost estimates, as they apply their program to the FCC, we'll see if that amount of money actually covers it or not.

Of course, the legislation also provides for unique ability to come back and identify additional resources.

Senator LEE. Just to be clear, does the Rip and Replace price tag as we've got it now take into account the increased cost of equipment resulting from it?

Mr. BERRY. The increased cost of equipment for?

Senator LEE. Resulting in fewer options when you're taking options off the table.

Mr. BERRY. Well, it's interesting. The timing may actually give you more options in the marketplace. Not only do we have the legacy of networks that are in place and you're replacing those legacy networks with probably existing, you know, vendors, suppliers that are in that work space, but you have new technologies coming onboard that, as time—if you can wait 9–10 months or a year, you may be able to reduce your costs.

So that's the unknown part and I think it's going to absolutely require a cooperative effort. We know what the goal is, to eliminate the equipment and the capability in the networks. How fast you get there will depend on how much cost it might cost.

Senator LEE. Thank you very much. Thank you, Chairman.

The CHAIRMAN. Thank you, Senator Lee.

Senator Peters.

STATEMENT OF HON. GARY PETERS, U.S. SENATOR FROM MICHIGAN

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

Mr. Boswell, this question is posed to you. With 4G, we have hardware choke points to check, maintain, and improve system security, but as we push to move from hardware to software in order to allow more U.S. companies to participate and take control of our supply chain, a question is can you describe how companies will have the same ability to check the cyber hygiene of software if there is no hardware choke point?

Mr. BOSWELL. Thank you, Senator. Yes, I would be happy to describe that, what we feel is a process certainly of top priority for Ericsson and my area of responsibility is security of our network products and integrity of our supply chain, and I believe that it focuses on three key pillars: transparency, traceability, and trustworthiness. I'll talk a little bit about each one, if that's OK.

Senator PETERS. Yes.

Mr. BOSWELL. From a transparency standpoint, so we do at the beginning code testing, vulnerability scanning, a privacy impact report, hardening guidelines, and other things on every release of code, and then we're very transparent in the process of how that and how we do that and those results are shared with the customers for all of those products, as well. So we're very open there.

On the traceability aspect, all of our software is scanned, verified, signed, and distributed in and from Sweden and that actually gives us a lot of tight control over our software development life cycle and the traceability of that supply chain with things like check-in and check-out procedures at the software level, and it provides a chain of software custody that ensures authenticity and integrity of the code once it has left Ericsson.

And then when it's deployed on a radio, for instance, with a customer and it boots up, they can be sure that that is verifiable and authentic code and it's going on secure and authenticated hardware, as well, because we put our certificates all the way down at the chip level of that radio. That gives us what we call a hardware route of trust all the way from the physical aspect of the radio to the software that's running on top of it.

And last, from a trustworthiness standpoint, of course, the trustworthiness of the network is going to be more than just the security and integrity of products. It's also operational procedures and transparency, how you do deployments, but also are you operating under the Rule of Law and under an independent judiciary. All of these things factor into determining trustworthiness of a vendor.

So we try to convey some of that information through things like the DHS Supply Chain Risk Management Task Force and giving guidance from a government and industry perspective to customers and carriers and enterprises and the rest of the world on here's things that we think make us secure and high-integrity supply chain.

Senator PETERS. All right. Thank you. Mr. Berry, certainly all the large network providers are building 5G and they're all committed to cyber and we hear that loud and clear.

My concern is that some small-and medium-sized wireless ISPs have fewer than 10 employees. Some of them can't afford to have a full-time cybersecurity officer around the clock, as you know.

So what recommendations do you have for Congress to incentivize small- and medium-sized wireless ISPs that serve our rural communities? How can we assist them so that they can have a robust cybersecurity program but maintain profit margins?

Mr. BERRY. Thank you, Senator. You're absolutely correct. That is a huge challenge for many of the small carriers serving, you know, isolated areas throughout the United States.

I think the bill does a phenomenal job of saying let's share information. Let's make sure that that information is shared with small providers. So CISA—which is the Homeland Security, they also are putting field offices out there and saying, listen, here's your contact. I would recommend that every carrier, whether it's WISP or a small wireless provider, know who those contacts are and most states have contacts and talk to them on a regular basis.

When the information gets out on this suggested list of providers and you have a Federal program through CISA, the Homeland Security, that can give you the data you need, you can get that, you should talk to them all the time and they will give you a head's up. They will let you know if this is a problem or if you are going to experience problems.

I've been very impressed with the new CISA operation. I think it's only a year or so in operation and they're doing a phenomenal job.

Senator PETERS. That's good to get that assessment. Is there more that they can do?

Mr. BERRY. Yes, I think there's more they can do, but I think the U.S. Government, in conjunction with industry, are doing a much better job of bringing some transparency to this issue. I was at a conference out in Miter, which is, you know, quasi-public/private entity, huge attendance from U.S. Government entities, and I was really surprised at the quality of data exchanged and the quality of interest from every military operation to the private sector, including many of the companies represented here.

Senator PETERS. Great. Thank you for your answer. Appreciate it.

The CHAIRMAN. Senator Sullivan.

STATEMENT OF HON. DAN SULLIVAN, U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Thank you, Mr. Chairman. I want to thank the witnesses for this very enlightening hearing and testimony, thank the Chairman.

Dr. Lewis, I want to talk a little bit about the issue of reciprocity with China. Senator Van Hollen and I last week introduced what is called The True Reciprocity Act of 2020, and as you know, in a whole host of areas, media, investment, economics, there's not a reciprocal relationship. They can do things over here that we can't do over there, and as you also know, Huawei, I mean, let's face it, I read the intel, they're clearly ultimately controlled by the Communist Party of China. Whoever says that's not the case doesn't know what they're talking about, and clearly subsidized.

But let me give you something that I find very disturbing that relates to reciprocity or the lack thereof and I'm wondering how we can address it.

Huawei has recently begun to file patent infringement lawsuits in the U.S. against its perceived or actual U.S. competitors, U.S. companies. So specifically they've filed a $1 billion patent infringement case against Verizon claiming over $1 billion in damages.

Could Verizon go to a Beijing court and file a patent infringement lawsuit against Huawei? I mean, everybody's laughing. What's the answer? Would they be treated fairly if they could? You can say no. I mean, I think I want to get to a broader point.

Dr. LEWIS. That's a quick answer. No.

Senator SULLIVAN. OK. Hell no?

Dr. LEWIS. Sure.

Senator SULLIVAN. OK.

[Laughter.]

Senator SULLIVAN. OK. But it's actually really an important question because in my view, they're using the openness of the U.S. society and our courts which are independent, theirs aren't, actually as a weapon against us.

So I'm just wondering not just for you but the rest of the panelists, the bill that Senator Van Hollen and I tries to say essentially if we can't do it there, you shouldn't be able to do it here. It is a broad category.

But should we look at, for example, maybe limiting discovery if—I mean, Huawei is going to try to use this not only to intimidate American companies but in the discovery process maybe try to get trade secrets, maybe try to get information from our tech companies, from our telecoms.

How should we be trying to address this because to me, this is a really big problem? They wrote a Wall Street Journal op-ed as if they're some kind of, you know, non-controlled party by the Communist Party, but do you have any thoughts on that, any of the other panelists, and then I have a quick question for Mr. Berry.

Dr. LEWIS. Let me start first, Senator, and thank you because this is a crucial issue.

Every time I open the *Washington Post* or last week's *Economist* and see an insert from *China Daily,* I feel like we are definitely being taken advantage of because the *Times* or even *The Economist* could not do that in China.

Senator SULLIVAN. So that's one of my elements and Senator Van Hollen's bills on the media side, right? It essentially says we can't go do that in China. Heck. You walk out of the Senate and you do a vote, you have a Chinese journalist sticking a mic in your face. Can our journalists stick mics in Xi Jingping's face? I don't think so.

Dr. LEWIS. This has been a long struggle over Chinese espionage and one of the things we've discovered is that if you close one door, our opponent will look to find another, and unfortunately I believe they use patents and discovery associated with patent cases as a new venue for espionage.

Senator SULLIVAN. And do you think it's threatening to the competitiveness of American companies to have to open up to broad-based discovery when there's no way they would allow us to do it in China?

Dr. LEWIS. I've only interviewed a few technology companies but all of them would agree with you that it's very damaging.

Senator SULLIVAN. Well, I will ask the other witnesses if you have a view on that and you want to submit it for the record, please do. I think it's a really important issue and it's a loophole.

Very quickly, I just wanted to ask Mr. Berry. I was part of the co-sponsorship of the Chairman's leadership on the Rip and Replace bill.

Can you speak to some of the other challenges dealing with mostly rural and extremely rural and remote carriers that Congress or the FCC can undertake as we are looking to implement the legislation that the Chairman led and we recently enacted in the Congress?

Mr. BERRY. Thank you, Senator. Yes, we mentioned accessibility is going to be the key to whether or not we get this done in a rational, reasonable way.

In Rural America, these carriers are literally working and operating on a shoestring and trying to keep connectivity while you're literally restructuring your entire network is going to require a lot of flexibility.

The FCC, you know, the last Order they did on USF, essentially Mobility One, there was some concern whether or not there was authority in there to be able to maintain your network while you're transitioning. Some of us thought that some of the provisions that the FCC had were retrospective in nature instead of prospective.

We all have to get on the same game card on this. If we're going to maintain the networks and provide services, especially in Alaska, it's so difficult in many areas, you're going to have to give a little flexibility to continue to maintain that network as you transition out.

So prioritization of how you do it and I think we're going to— just because a generator goes out on a network doesn't mean that it's a Huawei product. Yes, that generator may actually allow that network to operate. That may have some Huawei, you know, goods and product in it, but that's not the reason you're maintaining the network and so I think it's going to take a lot of cooperative effort and the rural areas are going to be one of the most difficult to deal with.

Senator SULLIVAN. Thank you. Mr. Chairman, I know that I'm the last witness. Can I just——

The CHAIRMAN. Actually, we have Senator Scott here.

Senator SULLIVAN. Oh, I'm sorry, Senator Scott. I'm not going to even finish my sentence then. I was going to ask for—I'll just have the witnesses, if you can submit additional comments on my earlier question about the lack of reciprocity and the——

The CHAIRMAN. You're going to be given an opportunity to say that aloud when I take my second round.

Senator SULLIVAN. Oh, well, maybe I'll hang out for that then. Great.

The CHAIRMAN. Senator Scott.

STATEMENT OF HON. RICK SCOTT, U.S. SENATOR FROM FLORIDA

Senator SCOTT. Thank you. Thank you, Chairman Wicker. Thank you, Senator Sullivan, for giving me this opportunity.

[Laughter.]

Senator SCOTT. Mr. Berry, could you talk about what we need to do to encourage private industry to create alternatives to Huawei because if you just read the paper, what you're reading, and when you talk to Europeans, they say, well, there are no alternatives and so what do we need to be doing to help create alternatives?

And then second, any of you can answer, if you're up here in D.C., we all understand the risk of Huawei, but the public doesn't get it. I mean, they don't hear it locally hardly at all and so on both these, what can we do to encourage and what can we do to get the public educated about the risk of Huawei?

Mr. BERRY. Thank you, Senator. I mean that's a tough one. What you can do to encourage is exactly what you did in the bill. You provided a fund for replacement equipment which means it got everyone's attention and, yes, everyone wants to find solutions now because there's a potential to pay for it.

Small carriers don't drive the marketplace normally. They don't drive the technology development. This gives us an opportunity to recognize that there are some funds to actually reimburse.

On the other side, I think the recognition that there's a nefarious, you know, network element out there that needs to be replaced gives everyone thought that maybe there's a better way to do it, and I think our industry has the capability to respond in a very effective fashion very quickly.

I think that's what we're seeing in the marketplace right now and many of those sitting at this table are providing that opportunity.

I know that small carriers really appreciate being able to know if they make a decision to go with a certain technology, it's on the recommended list. They're not going to literally have to go wonder because they can't pay the bill.

Senator SCOTT. And how can we educate people better?

Mr. BERRY. Well, it's a good idea. We did three nationwide sessions trying to educate our carriers to the risk and we had great response not only from Department of Justice, FCC, Homeland Security, NTIA, and the White House. Those are the types of things.

The big issue is everything's connected to the Internet and, you know, it doesn't matter if it's a switch, a part of the RAM, or part of the core, eventually it connects to the Internet and just because it may happen in

Washington, D.C., you could have a plant shut down in Florida because of that vulnerability. It's like the chain that breaks at the weakest link and I think that's what all these interesting discussions are trying to do right now is find that weakest link and fix it.

Senator SCOTT. When you all were answering Senator Sullivan's question, you talked about Huawei using the patent process to take advantage of the American system and probably other countries.

Is there anything that we should be doing to penalize Huawei for doing that? Is there anything through the patent process that we can do that would penalize them because companies like Ericsson and Nokia don't do that?

Mr. BERRY. For me, putting on my old hat as I used to be counsel to the House Intelligence Committee years ago, the nefarious thing about that is that open process, the best way to defeat that challenge is potentially through information that's classified and cannot be made public and that concerns me from my service on the Hill.

I don't know exactly how you do that in a public fashion, but that's a good way anyone can test the knowledge that the U.S. intelligence community may have by bringing actions like that and I'm not so sure I have a good answer for you.

Senator SCOTT. So is there legislation now that protects classified information like that that would——

The CHAIRMAN. Well, will you yield to Senator Sullivan?

Senator SCOTT. Absolutely.

Senator SULLIVAN. Well, I mean, what we're looking at is not the classified aspect but just the reciprocal aspect and the reciprocal aspect to me is glaring, particularly in this case, because our companies can't do that. So one response that's pretty much in the bill that Senator Van Hollen and I put forward is that you would limit discovery to Chinese companies in American courts because we can't do discovery in their courts. It seems very fair. Most Americans would, I think, instinctively support it.

If we get all of our allies to do the same thing, then you start to really leverage China to quit playing in a way that's non-reciprocal.

Senator SCOTT. But there's nothing else that from classified side that you have a recommendation that we need to be doing?

Dr. LEWIS. Well, Senator, one of the issues that's come up in this discussion, and it's true, the one way the Chinese leaders really dislike is reciprocity and so in discussions with Chinese officials, if you say reciprocity as a threshold, they are very unhappy.

We need to consider whether you can use some of the sanctions tools available, whether it's putting people on the entities list, whether there are other Treasury or Commerce sanctions that might offer an opportunity to close off this new avenue of espionage.

Senator SCOTT. Thank you. I think I'll stop. I think my time's up.

The CHAIRMAN. Thank you very much.

Dr. Lewis, Huawei is on the entity list, it cannot receive information from U.S. persons and entities, but it can sue and try to get around that through discovery and you and Senator Sullivan had a lenghty exchange about that.

Mr. Berry, is there anything more you'd like to say about this issue? Then I'll give our other three witnesses a chance to respond.

Mr. BERRY. No, sir. I think it's another way to glean information that would not otherwise have been made available and I agree with Senator Sullivan that it has to be addressed.

The CHAIRMAN. Would anyone else like to weigh in on that? I don't see anyone raising a hand.

Senator SULLIVAN. Chairman, can I just make one quick point——

The CHAIRMAN. Yes.

Senator SULLIVAN.—just to add to this discussion?

So when I raised the issue of reciprocity with the Chinese at very senior levels, including with our Ambassador here but also with senior officials in Beijing, it's one of the issues where they pretty much acknowledged that there's no reciprocal treatment across a whole host of areas, but they say that it's still appropriate that it's non-reciprocal because they're a developing country. That's literally the answer. That's what they say.

Obviously that's a debatable prospect, but I think true reciprocity in the relationship has to be the standard. We get our allies to do it, too, we can leverage China in a huge way because they don't have reciprocal relationships with hardly anybody.

That's my comment.

The CHAIRMAN. Thank you very much.

Now as we conclude, let me see if we can cover the Federal Advisory Committee. The Communications Security Liability and Interoperability Council that the FCC works through, I think we call it CSRIC, its mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems.

So, Mr. Murphy, can you discuss why 5G networks will require a different approach to communications network security compared to 4G and 3G, and then, Mr. Berry, I'm going to follow up by asking you concerning the security of the telecommunications supply chain. It requires diligence from operators to monitor their networks.

While there's no one-size-fits-all approach to address vulnerabilities, what types of best practices are your member companies adopting?

So, Mr. Murphy, would you care to help us on that issue?

Mr. MURPHY. Yes, thank you, Chairman Wicker. So 4G is largely dominated by smart phones. 5G will be dominated by smart phones and IOT devices and many different types of industries and some of those are critical industries.

Ranking Member Cantwell mentioned the power issue earlier this morning. So the potential for catastrophic impacts are larger in 5G. Likewise, the network itself is changing in the way it's structured, moving toward a more distributed system, more virtualized system. So we cannot take what was done in 4G and say that was adequate for 5G. We need to look at 5G as something that is new and has a higher bar for the security processes we implement.

So that's why we think, for example, this whole issue of trust of the supplier comes in to play. It has a more important aspect in 5G compared to 4G and likewise on the technical level, vendors, such as ourselves and Mr. Boswell with Ericsson, we also have to up our game in the security process we implement for 5G because it is not the same.

The CHAIRMAN. Mr. Boswell, you are going to have to up your game?

Mr. BOSWELL. Senator, thank you. Actually, I definitely would like to speak on this topic as I serve on the FCC's CSRIC that you had mentioned.

All of our customers are going to be going through a transition of some kind as they move into 5G and with this FCC Security Advisory Council, we're working on two different working groups right now. One of them is focused on stand-alone 5G security, the other is focused on—the one that I serve on is the transition from the other Gs into 5G and I think that's an area of extreme importance, especially for the smaller carriers.

The reason is the work that we're doing there is very collaborative, colleagues from Nokia, there are many others, government and industry. The lessons learned out of what we can do and the transition of 5G will be applicable not only for the large carriers but also for those small carriers because all of them will be in this transition state between 4 and 5G for quite a while.

It's important for us to provide consistent and predictable guidance on how do we update security policies and procedures to be ready for this new virtualized software-defined infrastructure.

For the smaller carriers in particular, that may be a completely new thing for them. The larger ones have been virtualizing things and doing some software-defined networking stuff for a while.

So they not only have the challenge of I've got to go put a radio on and figure out how to make that work and deliver new services but now I've got virtualized infrastructure, as well. That may be new for them.

So we're trying to address this in the FCC Security Advisory Council that you mentioned and we appreciate the work and the backing from the government that's set that up.

The CHAIRMAN. Mr. Berry.

Mr. BERRY. Thank you, Senator. I guess it's important to follow on that with its virtualized components or new portals are not inherently more secure in and of themselves. We learn how to make them more secure from actual experience and practices and that's where CSRIC and the engineers and the vast testing activities come in to play because you can share that information with carriers.

Most of the small carriers are trying and still impact their networks but, for example, if you go down to C SPIRE in Jackson, Mississippi, you go in their NOC, their Network Operations Center, they can tell you literally to the minute how many adversarial attacks they've had on the network. They can tell you how many intruders attempted to get into their network and communicate with, you know, entities in their network.

So some of our carriers are actually hiring outside third party entities that monitor through dark fiber and other types of scenarios everyone that's trying to touch their network. So it's a constant thing and without CSRIC and some of the other experience-oriented entities that are out there, our small carriers would have a very difficult time coming up with best practices because it changes, literally the threat changes literally every day in some respect.

So that's a key component and I think not only do you have to continue it but I think we're going to have to be probably even more energetic in response in the coming years.

The CHAIRMAN. Thank you. Dr. Lewis, something you said about partially using Huawei equipment might give someone the impression that you are somewhat relaxed about what the United Kingdom has done and so I'm just curious to learn what you really, really think there. I can handle the truth.

Dr. LEWIS. I am relieved to hear that, Mr. Chairman, and let me say that Congress has been the bedrock of the opposition to Huawei in the confrontation with China. So your work is much appreciated, and I think your comments about how I'm relaxed will please my friends in GCHQ. So we've got to look on the bright side.

It's an open debate as to whether you can do the divide that the British have talked about and the architectural fix. My issue is you have to play the hand you're dealt and that's the hand we've been dealt.

It would be better if they did what Australia did. They chose not to do that. They're our closest allies in the world. How do we work with them to make it a secure system?

They might change their mind. We have some leverage points, but for right now, like partial ban, not like partial ban, that's not the game. The game is how do we make our communications with a key ally more secure?

The CHAIRMAN. Three of our witnesses have said today that there are a lot of alternatives and apparently the U.K. is not convinced. They didn't get that message. Am I on to something here?

Dr. LEWIS. I would say that the U.K. received political direction possibly from the previous Prime Minister that it was important to maintain good relations with both China and the U.S., economic relations with China, security relations with the U.S., and the British are trying to craft a solution that will let them do both. That may not be possible, but I don't think the technical debate over whether their partial ban can work is over.

There are even American tech companies that will say with the right architecture, with the right setup in the cloud, you could make this work. So it's a to-be-determined kind of question.

The CHAIRMAN. Senator Johnson.

STATEMENT OF HON. RON JOHNSON, U.S. SENATOR FROM WISCONSIN

Senator JOHNSON. Thank you, Mr. Chairman. I've got a lot of questions, so succinct answers would be helpful.

Mr. Lewis, I appreciate your testimony. I was in Munich. Microsoft was talking about a cloud-based solution that just basically leapfrogs the, no offense to Nokia and Ericsson, the equipment issue when it comes to 5G.

I come at this from the standpoint of regardless what is best in terms of national security, the reality is Huawei's going to exist. There's 1.4 billion people in China, 400 million in the middle class. They got a good market and they're going to have equipment and somewhere around the world that equipment is going to be installed and in a global network, we're going to come in contact with it. So we need to recognize that reality.

Rather than, you know, trying to impose a policy that's not going to be accepted by everybody, we better accept the reality that we're going to have to come up with solutions that contemplate the reality that Huawei's equipment is going to be installed some places.

Can you speak to that, Mr. Lewis? Then I want to start talking to Nokia and Ericsson about manufacturing capabilities and capacities and that type of thing.

Dr. LEWIS. Thank you, Senator. I think that's right, unfortunately, that when you look at some of the markets in the developing world where we have strong national interests, the Middle East, Africa, South America, Huawei will be a presence there, and so we need to learn how to operate on networks that are not perhaps trustworthy.

We have an opportunity here, though, in the move toward 5G and to 6G to work with our allies, to work with our security partners to come up with standards and best practices that will make telecom more secure.

So I don't see the British decision as a loss. I see it as an opportunity.

Senator JOHNSON. Well, I view it as a reality. Speak to the cloud-based solution for 5G, you know, basically leapfrogging the equipment issue.

Dr. LEWIS. And I'll defer to my other colleagues, of course, but what I hear from interviewing many, many companies is that this is an alternative. It will lead to greater security, but it is somewhere between 3 years and 10 years out. So it would be nice if it was here sooner. It will fix our problems, make them smaller ultimately. Next year, it won't help.

Senator JOHNSON. So often here, you can't defeat something with nothing, but we have something. We've got Nokia. We have Ericsson. How big of a capacity challenge is meeting the demand for 5G as it develops and is deployed? I'll speak to both Nokia and Ericsson here.

Mr. MURPHY. I'm sorry, Senator Johnson. Cacacity in what respect?

Senator JOHNSON. Of the equipment that's needed to satisfy 5G demand and deployment.

Mr. MURPHY. Yes, so it?s growing at a different pace in different countries across the world, but at the moment, we don't see a significant issue with meeting the equipment demand.

There's a great demand on capabilities which is very challenging to meet. However, not so much on the equipment side.

Senator JOHNSON. But we're always told that Huawei's equipment is substandard, is that true or not true? Are they advanced or are they ahead of Nokia and Ericsson in terms of technology or on par or behind?

Mr. MURPHY. I think it would be false—I mean, it's correct to say that Huawei is a formidable competitor. That's partially due to the massive research and development arm they're capable of supporting due to their domestic market as well as support on the sales side from the banks in China.

However, when it comes from a technical perspective, if we go back to the earlier part of my testimony, if we look at first in the world, it's actually the U.S. was the first in the world to launch 5G back in the fourth quarter of 2018 and then more commercial systems in 2019 and we have many more firsts.

So we do not feel we're at a technical disadvantage in being able to keep on par with Huawei.

Senator JOHNSON. So China's predatory mercantilism, you're talking right now about being supported by, you know, Chinese banking. Is there a greater economic support from China? I mean, how large an economic disadvantage is Nokia and Ericsson? You know, how big a disadvantage is that to Huawei? I'll ask Mr. Boswell to answer that one.

Mr. BOSWELL. Thank you, Senator. So we certainly believe in the security and integrity of our network products and our solutions and we think they're the best in the world.

You asked about kind of a comparison to them. As Mr. Murphy said, they're a formidable opponent and certainly a competitor on the world stage. Here in the U.S. market, the U.S. enjoys a competitive and robust marketplace of secure and high-integrity and trusted suppliers, and I think it's important to uphold that as an example to the rest of the world.

We can still go really fast on this race to 5G and do it with secure and trusted suppliers.

Senator JOHNSON. No offense. You're not answering the question. I'm talking about what kind of cost disadvantage are you at, both your companies at because of China's mercantilism and their state-sponsored support. If it's just a matter of EXIM Bank financing this stuff, you know, that's not a big deal. If it's Russia or if it's China literally putting billions and billions of dollars into subsidizing the sale of the 5G equipment, that's a problem. So where are we at there?

Mr. BOSWELL. So my apologies, Senator. The finance side of that thing is not really my forte. I'm on the security and engineering side of our practices at Ericsson.

However, I would agree with what Mr. Murphy said about we're not facing restrictions in terms of our ability to meet manufacturing demand in terms of equipment and getting it out there and meeting the roll-out demands that our customers are asking for. That's both in the U.S. and in the rest of the world.

So we're able to go kind of as fast as our customers are wanting us to right now.

Senator JOHNSON. So if the Chairman would indulge me, can anybody answer that question in terms of the cost disadvantage we're at, anybody on the panel?

Mr. MURPHY. I can try. So ironically, 25 years ago, I moved to China at this time of the year, and I set up a research and development lab and in my lab were two companies called Huawei and ZTE, and they developed very rapidly obviously and they developed because of government support and the provinces purchasing their equipment and research and development done at a very low cost, if not free, by universities and government research institutes.

So that at that point in time, I believe that continues today. They have very significant support from the government and different entities within China in the execution of their product developments and subsequently in the sales through the financing mechanisms.

So we do have some disadvantages in that respect. We're not having equal level of support from governments to help us. So in a sense of what can be done to remediate that or mitigate that, I think it's to create a level playing field, both on the EXIM Bank-type things but also on the research and development side to support vendors like ourselves to have a more level playing field both in 5G and especially moving into 6G.

Senator JOHNSON. Well, we're not going to steal your technology in this, so I can't get an answer that they're 30 percent below you guys. I mean, I won't get that answer and again I've already taken more time.

Mr. Lewis, I just would like to meet with you at some point in time.

Dr. LEWIS. OK. You know, just a quick one on the———

The CHAIRMAN. Is that 30 percent accurate?

Senator JOHNSON. No. I was just picking that number out of the air.

Dr. LEWIS. There's some evidence that at least in one case with the European company, it was at 30 percent discount. In other cases, you know, it's been much greater. So we can answer that in our question, if you wish.

Senator JOHNSON. OK. So we'll do that offline. Thank you, Mr. Chairman.

The CHAIRMAN. Go ahead, Senator Johnson. This is interesting.

Senator JOHNSON. Oh, OK. So answer the question. We need to know that. If we're going to—and by the way, I mean, in the private sector, if you've got an incumbent supplier that has a monopoly that you want to get rid of, you start supporting alternative suppliers, and I think we're in the same situation here. We've got to—China has taken the wrong path. They're not a benign force. They're a malignant force. This is a national security issue. So we've got two suppliers here. We've obviously helped them here by saying we're not going to allow Huawei but we may need to do some support from the standpoint of competing against their predatory mercantilism, but we need to know what extent that is.

So again, Mr. Lewis, if you've got some information that would be helpful.

Dr. LEWIS. Well, perhaps this is best answered in a question for the record, but in conversations with both U.S. and foreign law enforcement and intelligence agencies, and I don't know if my colleagues would agree, they would tell you that if there's a Chinese interest in getting into that market and having access to the national telecommunications system, they would spend whatever it takes. So it's in hundreds of millions in some cases, greater in others.

Senator JOHNSON. By the way, that's the kind of competitor you don't like competing against. They'll buy the business at any price. OK.

Well, again, we will talk offline and do some questions for the record. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Johnson.

So, Dr. Lewis, it's not accurate to say that our allies who made a decision that we wish they had not had no one else to turn to? That's really not an accurate statement, is it?

Dr. LEWIS. That's correct, Senator. As you've heard from our colleagues from Nokia and Ericsson, there are many alternatives.

The CHAIRMAN. And I think that's an important take-away from this hearing and, Mr. Berry, do you want to have the last word?

Mr. BERRY. Thank you, Senator, appreciate it. To respond to Senator Johnson, this Committee sent a huge shot across the bow of every ally and friend to the United States. You said, this Committee said we are willing to share the cost and take the cost of ensuring our networks are secure. It doesn't matter what the covered equipment providers cost is or is not. They can't sell in the United States. They won't have a market in the United States.

So I think what you did on the international front is far more important than you may think. What you were willing to do here is what you wanted Britain to do, what you wanted Poland to do, France, all of our allies.

Now you have a barricade to stand behind and say can you follow our lead and I think that's what you've done here.

The CHAIRMAN. Thank you. It was actually a statement by the House and the Senate as a whole on a bipartisan basis and I expect the President will be signing that legislation with some fanfare in the next few days.

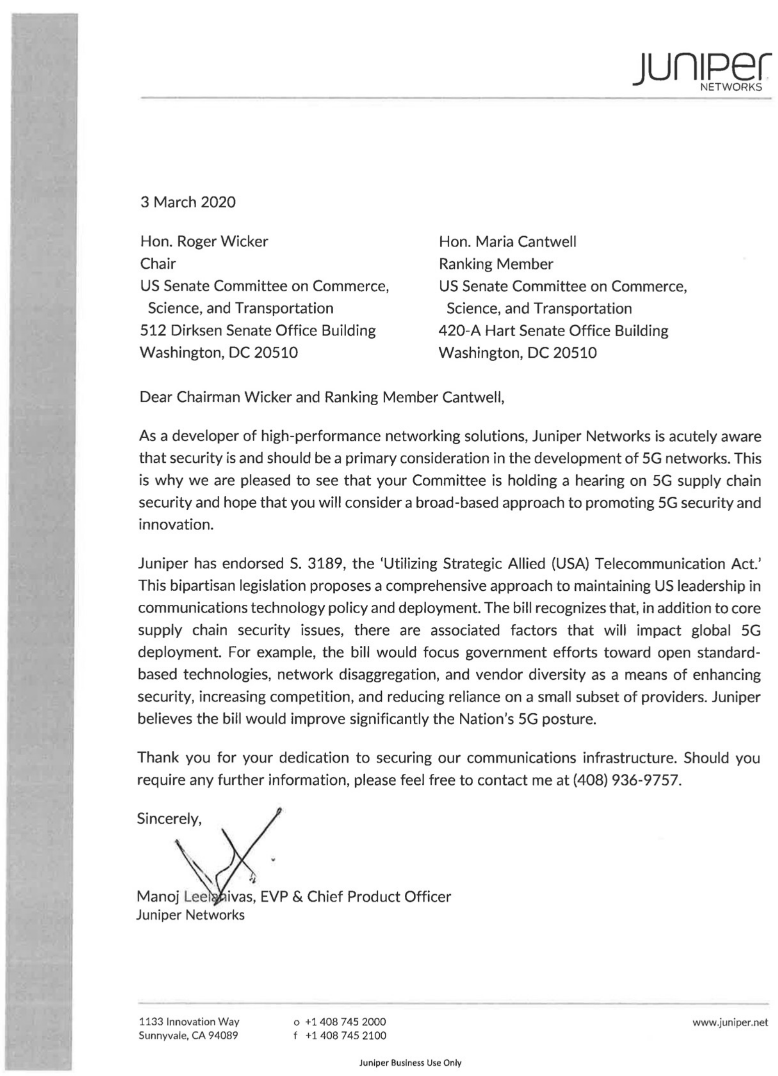
Thank you all, and I want to thank all of the members who have come and gone and I think helped us strengthen our understanding.

The hearing record will remain open for two weeks. During this time, Senators are asked to submit any questions for the record. Upon receipt, the witnesses are requested to submit their written answers to the Committee as soon as possible but by no later than Wednesday, April 1, 2020. Cross your heart, hope to die.

And so with that, I want to thank the witnesses and announce that this hearing is now adjourned.

[Whereupon, at 12:02 p.m., the hearing was adjourned.]

A P P E N D I X



JUNIPER
NETWORKS

3 March 2020

Hon. Roger Wicker
Chair
US Senate Committee on Commerce,
Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Hon. Maria Cantwell
Ranking Member
US Senate Committee on Commerce,
Science, and Transportation
420-A Hart Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell,

As a developer of high-performance networking solutions, Juniper Networks is acutely aware that security is and should be a primary consideration in the development of 5G networks. This is why we are pleased to see that your Committee is holding a hearing on 5G supply chain security and hope that you will consider a broad-based approach to promoting 5G security and innovation.

Juniper has endorsed S. 3189, the 'Utilizing Strategic Allied (USA) Telecommunication Act.' This bipartisan legislation proposes a comprehensive approach to maintaining US leadership in communications technology policy and deployment. The bill recognizes that, in addition to core supply chain security issues, there are associated factors that will impact global 5G deployment. For example, the bill would focus government efforts toward open standard-based technologies, network disaggregation, and vendor diversity as a means of enhancing security, increasing competition, and reducing reliance on a small subset of providers. Juniper believes the bill would improve significantly the Nation's 5G posture.

Thank you for your dedication to securing our communications infrastructure. Should you require any further information, please feel free to contact me at (408) 936-9757.

Sincerely,

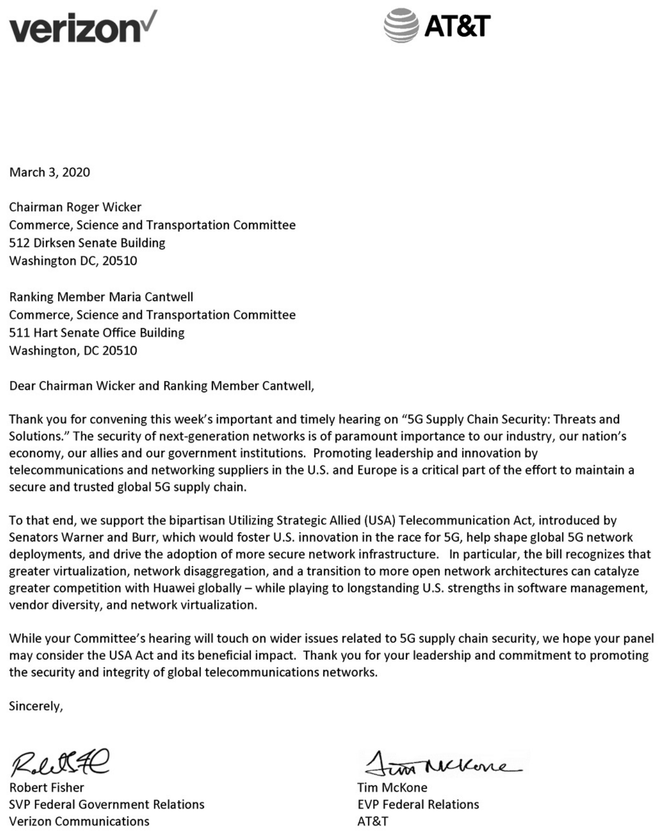
Manoj Leelanivas, EVP & Chief Product Officer
Juniper Networks

1133 Innovation Way
Sunnyvale, CA 94089

o +1 408 745 2000
f +1 408 745 2100

www.juniper.net

Juniper Business Use Only



verizon✓ AT&T

March 3, 2020

Chairman Roger Wicker
Commerce, Science and Transportation Committee
512 Dirksen Senate Building
Washington DC, 20510

Ranking Member Maria Cantwell
Commerce, Science and Transportation Committee
511 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell,

Thank you for convening this week's important and timely hearing on "5G Supply Chain Security: Threats and Solutions." The security of next-generation networks is of paramount importance to our industry, our nation's economy, our allies and our government institutions. Promoting leadership and innovation by telecommunications and networking suppliers in the U.S. and Europe is a critical part of the effort to maintain a secure and trusted global 5G supply chain.

To that end, we support the bipartisan Utilizing Strategic Allied (USA) Telecommunication Act, introduced by Senators Warner and Burr, which would foster U.S. innovation in the race for 5G, help shape global 5G network deployments, and drive the adoption of more secure network infrastructure. In particular, the bill recognizes that greater virtualization, network disaggregation, and a transition to more open network architectures can catalyze greater competition with Huawei globally – while playing to longstanding U.S. strengths in software management, vendor diversity, and network virtualization.

While your Committee's hearing will touch on wider issues related to 5G supply chain security, we hope your panel may consider the USA Act and its beneficial impact. Thank you for your leadership and commitment to promoting the security and integrity of global telecommunications networks.

Sincerely,

Robert Fisher
SVP Federal Government Relations
Verizon Communications

Tim McKone

Tim McKone
EVP Federal Relations
AT&T

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO STEVEN K. BERRY

Question. The Federal Communications Commission (FCC) estimates that it will cost more than $1 billion for rural carriers to remove and replace equipment and services from companies that pose a national security threat, such as Huawei and ZTE. In your testimony, you emphasized the importance of Federal funding for rural carriers that cannot afford to cover these costs and of ensuring that rural communities remain connected during the transition to secure 5G networks.

- In your view, are additional resources needed to ensure rural carriers remain connected during the transition to secure 5G networks?

Answer. Congress created the Secure and Trusted Communications Networks Reimbursement Program in the recently enacted Secure and Trusted Communications Networks Act to provide the additional resources needed to transition carriers away from covered equipment. While total costs will vary by carrier and depend on how different networks are structured, I am pleased that the FCC has sought $2 billion in resources for this program, as well as administrative costs, in a recent appropriations request.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JON TESTER TO STEVEN K. BERRY

Question 1. As you testified, the issue of suspect telecommunications equipment disproportionately affects small carriers in rural areas like much of Montana. For financial reasons, these carriers sometimes chose to use equipment that we now know to pose national security risks. What is the range of credible estimates for the total cost of replacing covered communications equipment among regional carriers, both in the "core" network and overall?

Answer. Each carrier's network is different, and accordingly resources needed to replace covered equipment will vary by carrier based on network architecture, current equipment in place, and size and density of each carrier's geographic footprint. The United States has never directed carriers to essentially remove all covered network equipment in one year or seek waivers, and the need for flexibility and ability to review new technologies that could reduce costs is extremely important. We hope the FCC recognizes this in their policy decisions, as technology advances and physical network components may differ in cost from virtual components. CoBank has estimated network costs to exceed $1 billion in network replacement costs, and the FCC recently sought $2 billion to fund the overall replacement program. To speak specifically to core costs, CCA carrier estimates approximate $3.7—$4 million per core, with additional costs for space to accommodate an additional core, expanded HVAC capacity, and configuration costs.

Question 2. Much of the covered equipment is obsolete, and will presumably be replaced by newer but functionally equivalent equipment, but the telecommunications market has only further consolidated in the short time since this equipment was installed. Are there proactive steps that could help ensure carriers have access to a robust and competitive market as they replace covered equipment? For example, do you anticipate that radio access network virtualization can play a role in replacement?

Answer. As you note, there are certain covered network elements that support legacy technologies that are now obsolete and no longer available from any trusted supplier. Carriers who must replace covered network elements should be allowed to deploy equipment to support like-for-like services, particularly with equipment that can be upgraded to support future technologies. Virtualization, including through Open Radio Access Network (ORAN) technologies, has the potential to disaggregate functionality to increase efficiency and decrease costs. Further research and development on ORAN should be encouraged. However, policymakers should not mandate which technologies are used in wireless networks, but rather encourage research into new, secure technologies to enhance innovation, customer choice, and cost savings. Superior products will win in the market.

Question 3. Are there currently enough skilled workers available to replace covered equipment in American networks within the specified timeline of one year after disbursement of funds? What steps can Congress take, if any, to help ensure the necessary workforce is in place in advance of the release of funds?

Answer. A properly trained, local workforce will be essential for impacted rural carriers to complete the transition process to remove covered network equipment; absent an appropriately trained workforce, there will not be enough labor available to complete not only the replacement of covered equipment but also other demands to wireless service deployment. I thank you for your leadership in introducing S. 3355, the Telecommunications Skilled Workforce Act, alongside Senators Wicker, Thune, Moran, and Peters to help meet the needs associated with bringing connectivity to rural America.

Response to Written Question Submitted by Hon. Amy Klobuchar to Jason S. Boswell

Question. In your testimony, you state that the United States is expected to account for 50 percent of data breaches across the globe by 2023, making our networks a target for cyberattacks. You also highlight the need for industry to develop 5G supply chain and security standards.

- Can you speak to how the industry is working together to develop 5G supply chain and security standards to ensure that all carriers, including small and rural carriers, remain competitive?

Answer. Security is a top priority for Ericsson. Ericsson's philosophy is that networks must, from the very start, be trustworthy, resilient, and secure by design, and Ericsson employs a holistic approach to ensuring the security of its supply chain and its products, as detailed in my testimony. At the same time, Ericsson and other companies in the information communications and technology (ICT) sector recognize that ensuring security in the 5G era is a shared challenge that requires collaborative and inclusive solutions. Accordingly, Ericsson constantly works with a diverse range of relevant stakeholders in industry and government—both in the U.S. and globally—through a variety of complementary organizations and processes to address 5G supply chain and security standards. This multi-faceted approach ensures that all providers—regardless of their size, the nature of their customer base, or other differentiating factors—are able to participate in the problem-solving process and, in particular, that the interests of small and rural carriers are taken into account.

Industry-led initiatives. Ericsson actively contributes to a number of U.S.-based industry initiatives organized around ensuring supply chain security. As described in my testimony, these include the Communications Sector Coordinating Council (CSCC), which meets regularly to review industry and government actions on critical infrastructure protection priorities in order to improve the physical and cyber security of sector assets, among other functions; and the Council to Secure the Digital Economy (CSDE), which brings together companies from across the ICT sector to combat increasingly sophisticated and emerging cyber threats through collaborative action.

Standards-setting bodies. Standards work is a foundational component of good security assurance, as it supplies guidance and frameworks that ensure security and privacy requirements are met consistently. As described in my testimony, Ericsson is a leading participant in developing the standards for 5G security through the global 3rd Generation Partnership Project (3GPP) and serves on multiple working groups within the standard-setting organization the Alliance for Telecommunications Industry Solutions (ATIS), including a newly-launched effort through ATIS, supported by the Department of Defense, to develop standards for securing the 5G supply chain. These technical standards are crucial for security because they give all suppliers and carriers a common—and open and transparent—technical understanding of interoperability and security. This allows for vetting and identification and correction of technical vulnerabilities. To be clear, 5G security standards and 5G supply chain standards are presently still under development, and Ericsson along with many other companies is helping shape them for long-term security. In total, Ericsson is a member of more than 100 industry organizations, standards bodies, and other technology alliance groups, as part of its mission to drive 5G forward.

Commercial partnerships. Ericsson further contributes to enhancing security through commercial relationships with its broad and diverse U.S. customer base, which includes nationwide and regional communication service providers serving both rural and urban markets with all technologies (wireline and wireless telecommunications, cable, and satellite). As described in my testimony, Ericsson has partnerships and collaborations with rural Wireless Internet Service Providers (WISPs) and carriers—such as GCI Communications, Cellcom, Bluegrass Cellular, and many more—in furtherance of its commitment to bring 5G to rural areas. Ericsson also maintains strategic partnerships with NVIDIA, Intel, Qualcomm, Juniper, and many other U.S. companies. In fact, Ericsson's global sourcing of active components for Ericsson's 5G radio base stations relies up to 90 percent on U.S. technology suppliers.

Industry-government initiatives. Industry and government together have convened numerous initiatives to promote collaboration on supply chain security. For instance, as explained in my testimony, Ericsson is involved in the following:

- The *Department of Homeland Security Information and Communications Technology Supply Chain Risk Management Task Force* exemplifies how industry and government collaboration can quickly and effectively deliver useful, sharable, expert-driven guidance in complex areas like supply chain and 5G security. The Task Force represents a formal, action-oriented collaboration between industry and government that ties together various streams of activity. In 2020, its working groups will analyze mitigations and risk determination across multiple areas of the supply chain in order to make recommendations on best practices and methodologies, and develop attestation frameworks around various aspects of supply chain risk management to help security standards and other risk guidelines more understandable, predictable, and useful.
- The *National Security Telecommunication Advisory Council (NSTAC)* is an industry-comprised body that advises the President on national security and emergency preparedness issues.
- Similarly, the *Communications Security, Reliability, and Interoperability Council (CSRIC)* is an industry-comprised body that makes security policy recommendations to the Federal Communications Commission (FCC). Three of its current working groups are expressly focused on security issues: Managing Security Risk in the Transition to 5G (WG2); Managing Security Risk in Emerging 5G Implementations (WG3); and 911 Security Vulnerabilities during the IP Transition (WG4).

Other engagement with government. Beyond these joint activities, individual companies work closely with other government departments and agencies. In Ericsson's case, these include the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST), both within the Department of Commerce; the FCC; the White House, and more specifically, the Office of Science and Technology Policy (OSTP), the National Economic Council (NEC), and the National Security Council (NSC); and the Departments of State, Defense, and Energy.

Collectively, these complementary vehicles and processes invite and permit the participation of all stakeholders, including small and rural carriers, and thereby facilitate holistic solutions to shared security challenges. In short, ongoing industry efforts are designed so that no stakeholder is left behind in the race to a secure 5G world.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KYRSTEN SINEMA TO ASHA KEDDY

Question. As you know, the Intel Future Skills initiative works to address the effect of technological advancement on the skills needed for the jobs of the future.

In order to compete and stay ahead of Chinese technologies, we must make significant investments in infrastructure, education, and workforce training. In Arizona, we are already working to cultivate a 21st century workforce. For example, last year Arizona State University and Sprint partnered to create a new 5G connectivity and Internet of Things curriculum.

How can we work to best prepare students for the jobs needed to build 5G equipment and networks in order to reduce provider dependence on cheap, Chinese components?

Answer. Intel commends and supports efforts to increase investments in infrastructure, education and workforce training. In passing the CARES Act during March 2020, Congress took important steps to protect early momentum to focus on these needs, and Intel supports additional resources for these important areas in follow up COVID19 response measures. In these uncertain times, one certainty is that the U.S. has an opportunity to set priorities for success against the country's most important challenges.

Today Congress has a rare opportunity to direct resources in ways that support the efforts of U.S. workers to develop new skills and begin building for the long term. Intel urges the Commerce Committee and Congress to learn from the example of Arizona's forward-looking plans. For example, in 2018 Arizona formed the Institute for Automated Mobility to advance readiness for automated vehicles. This effort will help advance technology readiness and regulatory frameworks for one of the most important applications of 5G technology. Especially during this time of pandemic, it is imperative to keep students and teachers connected to mitigate some of the disruption. That's why Intel announced the Intel Online learning initiative to support education-focused nonprofit organizations and business partners to provide students, without access to technology, with devices and online learning resources. In close partnership with public school districts, the initiative will enable PC donations, online virtual resources, study-at-home guides and device connectivity assistance. The Intel Online Learning Initiative builds on Intel's long-standing commitment to technology that improves learning. Although Intel's broad efforts were driven by a desire to support students, health care professionals and businesses of all sizes during the COVID–19 pandemic, Intel has strategically aligned its support with the goal of driving long term innovation against the world's greatest challenges (for more information on Intel's efforts, the press announcement is located at the website *https://newsroom.intel.com/news/intel-commits-technology-response-combat-coronavirus/gs.3a0m7n.*

As a leading provider of technology to 5G infrastructure, an employer of tens of thousands of the engineers who are inventing the amazing experiences of the future, and as the world's leading semiconductor integrated device manufacturer, Intel Corporation welcomes the opportunity to advise and support efforts to ready infrastructure, education and workforce in the U.S. for success in the 21st century and beyond.

Response to Written Question Submitted by Hon. Kyrsten Sinema to Dr. James A. Lewis

Question. Arizona has led the way in developing and deploying the technologies of the future. In 2019, two major carriers launched 5G services in the Phoenix area, bringing Arizona families and companies enhanced networks, greater connectivity, and the economic opportunities that go alongside. However, greater connectivity also means greater access to Arizonan's private personal information and propriety data.

There seems to be debate over the threats posed by equipment used in the core network verses non-core parts.

Is there a security threat posed by Huawei and ZTE in non-core parts of U.S. networks? If so, how great is the threat?

Answer. Chin is perhaps the most aggressive intelligence opponent the U.S. has ever faced. This means that any Chinese technology that connects back to a Chinese company could be exploited for espionage purposes. Chinese law makes any Chinese company a tool for Chinese espionage.

Huawei, with its longstanding and close ties to the Chinese government, falls into an especially high category of risk. The only way to completely eliminate risk is to not use Huawei equipment. Some countries argue that for the next few years as we transition from 4G to 5G networks, it is possible to manage the risk of using Huawei equipment through partial bans that limit the use of Huawei. These countries share the U.S. assessment of the risk of using Huawei, but argue that they can mitigate risk (but not eliminate it) to an acceptable and manageable level by restricting the use of Huawei equipment to limited part of the 5G network.

The United Kingdom, for example, uses a partial ban to exclude Huawei equipment from "sensitive" areas and its use confined to the edge. There is much debate over whether this partial ban is enough to mitigate the risk of using Huawei equipment. 5G networks will perform many operations once done in the core at the edge, which will have the increased computing power. Edge computing is part of what provides 5G with higher speeds, and this also means that keeping high-risk suppliers out of the core does not end all opportunities for espionage and disruption.

The UK argues that careful network architecting and greater attention to cybersecurity can overcome this risk. In the U.S., where many smaller networks still use Huawei equipment, there is less risk, as this is older technology, but since these companies did not design their network for security and may not have the best cybersecurity tools available, using Huawei create espionage opportunities. China will try to find ways to use this Huawei technology to collect information from the network on which it is installed and attempt to use it to gain access to other larger networks. The only way to eliminate risk is to eliminate Huawei technology.