CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

CHRISTOPHER D. ROBERTI
SENIOR VICE PRESIDENT
CYBER, INTELLIGENCE, AND
SUPPLY CHAIN SECURITY POLICY

1615 H STREET, N.W.
WASHINGTON, D.C. 20062
(202) 463-5449
CROBERTI@USCHAMBER.COM

June 25, 2020

Mr. Travis Hall
Telecommunications Policy Specialist
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Dear Mr. Hall:

On behalf of the U.S. Chamber of Commerce, I am pleased to provide these comments to inform the development of the implementation plan for the *National Strategy to Secure 5G*.

We believe that fifth generation wireless technology (5G) offers the potential for significant benefits to consumers, businesses, research institutions, and governments worldwide, many of which will only become apparent as 5G networks are deployed and utilized. These benefits undoubtedly will help to drive economic growth for the next decade. That said, the promise of 5G only will be fully realized in the United States if the U.S. government continues to support the private sector's deployment of 5G through a coordinated and comprehensive strategy that leverages the government's strengths in overcoming unfair competitive practices, ensuring robust deployment, adopting secure networks, and managing the risks to our economic and national security. Accordingly, the Chamber urges the U.S. government to take the following actions:

1. Support investments in research.
2. Uphold fair processes in standards-setting bodies.
3. Accelerate deployment of all technologies that will support the 5G ecosystem.
4. Provide strong intellectual property rights for innovators.
5. Help allies see a larger market for trusted vendors.
6. Facilitate the transition to interoperable technology-neutral solutions.

The Chamber, together with our members, is heavily invested in a successful rollout of 5G wireless communications systems and networks in the United States. This generation of communication systems is the most advanced and secure system deployed to date. The faster speeds, higher bandwidth, and lower latency of 5G (fiber-enabled) networks, have the potential to enable and support a wide range of applications (*e.g.*, autonomous vehicles, remote surgery, virtual reality and the Internet of Things (IoT), and others), far beyond what current networks can support. The private sector currently is deploying these networks in a manner that includes procedures to identify, manage, and mitigate attendant risks that arise from next generation technologies applied in novel ways.

Governments—including the U.S. government—are appropriately orienting themselves to address these risks, which include the availability and integrity of networks; the security and resilience of the supply chains that support them; and confidentiality and privacy of data that flows over and through them and is stored on them. Our members share the U.S. government's concern that there is no place for untrusted vendors in any part of 5G networks, *i.e.*, in the core, radio access network (RAN), or edge. Further, we believe that the U.S. government and its traditional international allies can – and must – foster trust and improve security through continued engagement with the private sector on technical and nontechnical risk identification and mitigation efforts, as well as the promotion of continued development of trusted 5G technologies, services, and products.

The Chamber acknowledges and appreciates the robust efforts underway within the U.S. government, including: (a) the White House *National Strategy to Secure 5G;* (b) the work of the National Economic Council to develop 5G software and other trusted 5G infrastructure; (c) the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) *Overview of Risks Introduced by 5G Adoption in the United States;* (d) the National Institute of Standards and Technology's (NIST) program *Preparing a Secure Evolution to 5G*; and (e) the leadership in advancing 5G spectrum issues by the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC).

In addition, the leadership of the National Security Council, U.S. Department of State, and CISA in working with allied foreign governments was critical in the negotiation and adoption of The Prague Proposals, in which the participating governments agreed on a set of recommendations to focus collective action to drive policies that ensure the deployment of secure and trusted 5G networks. Similarly, the common international approach to security is evidenced in the European Union's *Cybersecurity of 5G networks EU Toolbox of risk mitigation measures*, which included technical consultations with the U.S. government. We recognize the U.S. government for its international engagement and leadership and look forward to future engagements.

The implementation plan for the *National Strategy to Secure 5G* must continue to utilize a whole-of-government approach to the deployment and implementation of 5G networks, draw on the deep resources and working groups across the U.S. government, and tap the expertise resident in the private sector to inform this effort. We urge the U.S. government to organize an interagency policy development process that aligns and focuses its various 5G initiatives and strategies across agencies, with input and feedback from the private sector.

The U.S. government should ensure that 5G networks are resilient against threats to its availability and integrity while protecting the confidentiality of the network. We support federally-funded 5G test beds to enhance the ability of 5G to be leveraged for national and homeland security purposes. Such projects should be time limited and not run in perpetuity. These initiatives would demonstrate progress and help industry and government test new solutions. By defining a desired end state and letting industry innovate to that desired outcome, government agencies will spur a virtuous research and development cycle.

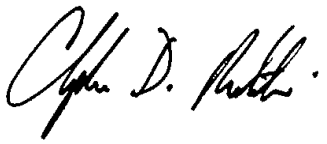
A main thrust of policymaking over the past few years is on the mitigation of threats of certain high-risk vendors (HRV) in the marketplace. The Chamber cautions the administration against policies that create artificial impediments to a vibrant marketplace merely for the sake of increasing domestic manufacturing capability. As we have said previously, it is imperative that

America win the global race to 5G and close the digital divide here at home. Passage of the Secure and Trusted Communications Act (P.L. 116-124) earlier this year made meaningful progress toward establishing a fund with the FCC to replace certain HRV equipment in previous generations of rural wireless networks. And we look forward to working with Congress, the FCC, and the National Telecommunications and Information Administration (NTIA) on implementing a flexible, fully funded replacement plan that emphasizes investment in next generation infrastructure.

As the U.S. government further develops its implementation plan and considers new initiatives, the Chamber urges the U.S. government to continue leveraging the multi-stakeholder process that has underpinned the development of global internet policy. The Chamber also urges governments at home and abroad to bring a full spectrum of industry stakeholders together for rich discussions on threat and risk assessments and mitigation measures (strategic and technical). Our experience is that consensus-oriented, technology-neutral, and industry-supported policies and a clear and coordinated interagency policy development process offer the best approach and are scalable to meet the global challenge.

As we have stated, it is imperative that America win the global race to 5G and close the digital divide at home. Detailed responses to the four lines of effort follow in the attachment. Thank you for your consideration of these recommendations. We look forward to working with you and your colleagues across federal agencies and with our international partners.

Sincerely,



Christopher D. Roberti

Enclosure

Line of Effort One: Facilitate Domestic 5G Rollout

(1) How can the United States (U.S.) Government best facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, network providers)?

A. Funding

Sufficient funding is critical to any discussion of securing 5G. While the private sector is best positioned to lead the domestic rollout of 5G and other communications technologies, there are approximately 27 million Americans without access to high-speed internet—particularly in the rural areas of our country. The Chamber asserts that the private sector is best positioned to lead the domestic rollout of 5G and other communications technologies. The private sector's leadership contributed to the U.S.' leadership in 4G, which has contributed over $100 billion annually to the nation's GDP.

Accordingly, the administration should work with Congress to fully fund the Secure and Trusted Communications Networks Reimbursement Program, which will be administered by the FCC as directed under the bipartisan Secure and Trusted Communications Networks Act of 2019 (P.L. 116-124). This will help U.S. firms remove vulnerable equipment and replace it with secure and trusted alternatives.

The nation's robust private communications sector has enabled the country to weather capacity-wise the shift to working and learning online. The administration should work with Congress to fund from general appropriations the deployment of technology-neutral, nonduplicative infrastructure for truly unserved areas. Regarding wireless communications, the administration should work with Congress to support collocation by enabling the leasing of tower space in addition to mere capital expenditures.

Additionally, the administration should work with Congress to provide tax credits to offset business expenses for rolling out commercial 5G systems in order to not pick winners or losers on specific technology or architecture choices.

B. Permitting

Funding alone will not address deployment of broadband, particularly 5G, without functional permitting systems. For example, unreasonable fee structures and delayed answers to permitting requests hinder the deployment of 5G. Further, localities generally require communication providers to pay for the installation of equipment on public rights of way (PROW). Unfortunately, these fees can exceed thousands of dollars in up-front application and administrative fees before even accessing a PROW. Local governments need to adopt rationale application processes that allow local concerns to be considered without unwarranted or unnecessary delays in the deployment of 5G.

In 2018, the FCC adopted an order that established shot clocks for localities to make decisions about small cell siting applications, in addition to requiring that the fees for siting small cell equipment be reasonable. The Chamber supported this order and the continued work of the commission to provide certainty to the permitting process.

The administration should also work with Congress to provide permanent permitting relief. For example, legislation like S. 3157, the STREAMLINE Act is a good start to improve siting rules. Wireline broadband also needs permitting reform to better connect all Americans.

C. Spectrum Policy

The federal government must develop a comprehensive, unified, national spectrum management strategy to reduce the artificial scarcity of spectrum and enhance the availability and flexibility in licensing and allocating licensed spectrum, while supporting international free trade agreements and access to international markets. Such a strategy should rely on market forces to determine the most efficient and effective uses for commercial spectrum, at the same time providing for other uses of spectrum in the public interest.

Additionally, preserving and encouraging the use of unlicensed spectrum technologies such as Wi-Fi is critical to the success of 5G and next-generation wireless networks. Wi-Fi is integral to the U.S. economy and will only become more so with the accelerated deployment of 5G, as new industrial and enterprise deployments leverage Wi-Fi hotspots to offload 5G mobile traffic. According to one report, the unlicensed spectrum that supports Wi-Fi contributed $525 billion to the U.S. economy in 2017, a figure that is expected to increase to $834 billion in 2020.

(2) How can the U.S. Government best foster and promote the research, development, testing, and evaluation of new technologies and architectures?

The administration should work with Congress to provide tax credits for research and development (R&D). It should also promote fundamental research through university and existing federal research grants (e.g., the National Science Foundation and the Defense Advanced Research Projects Agency). A non-exhaustive summary of these R&D initiatives, which would advance the U.S. government's goals and industry's drive for innovative solutions, include the following:

- 6G Advanced Research projects.
- Department of Defense 5G research collaboration and advanced prototyping.
- Ecosystem innovation on 5G platforms through sophisticated industry partnerships.
- 5G supply chain capabilities, such as manufacturing and advanced service delivery capabilities.
- 5G product development focused on integrated open network architecture, cloud RAN, network exposure, orchestration, AI, and edge computing.

To ensure that these initiatives are coordinated across federal agencies and are outcome focused, the administration should establish a task force with private sector participants to develop policies that foster a vibrant and diverse 5G supply chain.

(3) What steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development, and testing?

See answers to questions 2.

(4) What areas of research and development should the U.S. Government prioritize to achieve and maintain U.S. leadership in 5G? How can the U.S. Government create an environment that encourages private sector investment in 5G technologies and beyond? If possible, identify specific goals that the U.S. Government should pursue as part of its research, development, and testing strategy.

The federal government should focus on fundamental research with a longer-term view toward development of intellectual property that will guide the development of the next generation (e.g., 6G and beyond) technology. Fundamental research and the resulting intellectual property enabled 5G and are critical to innovation in the business community. Indeed, our overseas competitors are investing hundreds of billions of dollars into 6G and beyond technology. If we continue to look at where we are today and not where industry is going, we will fall further behind.

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure.

Broadly, the Chamber recommends that the federal government continue to support the efforts of the numerous industry bodies—including the 3rd Generation Partnership Project (3GPP), the Alliance for Telecommunications Industry Solutions, and the Council to Secure the Digital Economy—as well as the public/private partnerships led by the National Institute of Standards and Technology, the Federal Communications Commission, and the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, among others that advance solutions to the various 5G security concerns. Gaps will continue to be identified in 5G deployment, though security will always be an iterative process. But the federal government should continue to support these bodies and partnerships that are building upon the lessons from previous generations of wireless and draw upon the collaborative efforts to enhance security standards as events merit.

Specifically, the Chamber recognizes the work of NTIA in identifying issues where there is a clear need for government action regarding the areas of spectrum, permitting, and supply chain vendor diversity. Moreover, the Chamber recognizes the work of the Communications Security, Reliability, and Interoperability Council (CSRIC) VI and VII, which did and are looking into 5G security standards leveraging the work at 3GPP System Aspects (SA) Working Group 3, which is responsible for determining security and privacy requirements, and specifying the security architectures and protocols.

Businesses share the goal of the U.S. and foreign governments to mitigate security risks to 5G infrastructure and are committing significant resources to the security and resilience of these networks. Many agree that inflexible, point-in-time regulatory requirements cannot possibly keep pace with malicious threat actors. Similarly, overly procedural security compliance mandates are costly, time-consuming, and ineffective, and divert organizations' limited resources away from increasing security and toward "check-the-box" compliance. The Chamber will continue to seek out effective risk-based security frameworks, while opposing regulations that elevate process over effectiveness.

Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

(1) What opportunities does the deployment of 5G networks worldwide create for U.S. companies?

5G networks use more components, both hardware and software, than previous generations of wireless networks. The Chamber appreciates the public comments by the director of the National Economic Council and economic councilor to the president Larry Kudlow earlier this year when he said that American leadership in software services could be leveraged under a common engineering standard that would enable traditional equipment manufacturers, software services companies, and new market entrants to succeed in the 5G marketplace. Such an approach should be technology neutral and enable the market to gravitate to the next generation of communications systems.

(2) How can the U.S. Government best address the economic and national security risks presented by the use of 5G worldwide?

As previously discussed, security of the 5G system is a function of a vibrant ecosystem of market participants, including the core and RAN infrastructure, edge devices, and standards.

(3) How should the U.S. Government best promote 5G vendor diversity and foster market competition?

The administration should work with Congress to enact the Communications Technology and Security Innovation Fund of the Intelligence Authorization Act for Fiscal Year 2021 (S. 3905). This legislation would establish a $750 million fund jointly administered by the secretary of Defense and the director of National Intelligence, with the funds available for 10 years to support research and the commercial application of secure and trusted telecommunications technologies in key international markets.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G.

(1) How can the U.S. Government best lead the responsible international development and deployment of 5G technology and promote the availability of secure and reliable equipment and services in the market?

The Chamber supports the Prague Proposals endorsed at last year's Prague 5G Security Conference. These recommendations were developed by cybersecurity officials from multiple countries, linked by common interests and collective activities, to counter threats and provided recommendations for nations to consider as they design, construct, and administer their 5G infrastructure. The Prague Proposals emphasize the need for 5G networks to be constructed based on free and fair competition, transparency, and rule of law, and they were recently personified in the U.S.-Poland Joint Declaration on 5G. We welcome the international collaboration embodied in the process that led to the initial Prague Proposals and look forward to future engagement.

(2) How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies?

The national standards strategy should be clear and reflect the market-driven principles of the American free enterprise system, optimizing efficiency and innovation. The U.S. benefits when industry and the federal government effectively influence the development or revision of international technology standards. The smart development of international standards for 5G deployments advances U.S. commercial and security priorities by facilitating constructive outcomes—including improved interoperability, greater trust in online transactions, and strengthened competitiveness of American products and services. U.S. companies should be able to fully participate in standards bodies, without concern over participation in meetings that are also attended by companies on the Entity List. Additional clarification by U.S. government is needed to sustain US leadership in important technology areas, including 5G.

A private sector-driven approach to standards is particularly suited to 5G and the digital economy in general. We urge the federal government to balance the needs of both government and private business stakeholders and devote more resources to the promotion of industry leadership in the development of standards, intellectual property, and patents that are essential to the deployment of an open technologies-based, secure, and trusted 5G ecosystem.

We recommend that the U.S. government play a convening role with industry to ensure appropriate representation at critically important standards-setting bodies and organizations. Additionally, we recommend that the U.S. government promote the international development and voluntary use of new standards that are open, technically sound, technologically neutral, performance based, and suitable for the purposes of the U.S government and industry.

The Chamber also recommends that the U.S. government regularly engage with the private sector outside of the standards development activities. This would help ensure that relevant stakeholders (e.g., U.S. government and the private sector) maintain awareness of progress, concerns, and strategies and would serve to displace any incorrect information about ongoing efforts. Also, while the U.S. government traditionally engages in standards development when it has procurement interests or technical expertise, agencies should also consider engaging in standards activities to support their objective of enhancing national and economic security.

(3) What tools or approaches could be used to mitigate risk from other countries' 5G infrastructure? How should the U.S. Government measure success in this activity?

It is important to recognize industry-led risk mitigation initiatives and standards activities. These activities are already contemplated in the 5G standards development process at the 3rd Generation Partnership Project (3GPP), specifically through SA WG3, which is responsible for determining the security and privacy requirements and specifying the security architectures and protocols. The smart development of international standards for 5G deployments, such as the 3GPP and progress by the Open Radio Access Network (O-RAN) Alliance, advance U.S. commercial and security priorities.

The Chamber is aware of clean path or zero-trust network concepts, including the U.S. Department of State's 5G Clean Path Initiative, which seeks to build an end-to-end communication path that does not use any 5G transmission, control, computing, or storage equipment from untrusted vendors. Zero-trust networks, which are becoming more common in practice, mean any system an operator connects with is considered untrusted regardless of the source. The operator puts a variety of technical controls in place to prevent that network from impacting the operator's availability and integrity. Practices like these are becoming more common, and industry-led approaches lead to common, open architecture, and standards interfaces and are the most effective models to accelerate innovation and open market competition.

The federal government should establish clear public policies aimed at accelerating the development and voluntary adoption and use of open and interoperable 5G technologies and solutions both domestically and internationally, particularly for the O-RAN standard. Open standards are developed through a recognized industry-led, consensus-driven solution and establish protocols and form foundations that make applications more functional and interoperable. The O-RAN standard not only streamlines the development and deployment of open technologies-based 5G, but it removes barriers stemming from vendor lock-ins that impede data exchange and interchange. The O-RAN standards will lead to an interoperable, software-defined network architecture and will benefit consumers, competition, the economy, and national security.

(4) Are there market or other incentives the U.S. Government should promote or foster to encourage international cooperation around secure and trusted 5G infrastructure deployment?

Public trust in 5G technologies is necessary to advance responsible development, deployment, and use. The speed and complexity of technological change, however, mean that the U.S. government and other governments cannot foster secure and trusted 5G infrastructure deployment alone; a partnership between governments, the business community, and other stakeholders is needed to pursue deeper coordination and collaborative innovation. International collaboration should look at a strategy that promotes market competition and diversity of 5G options. Additionally, R&D is not confined by national borders, and the Chamber urges international collaboration.

Fostering secure and trusted 5G infrastructure can be strengthened by leveraging the Export-Import Bank of the United States' (EXIM) financial products to directly neutralize export subsidies offered by the People's Republic of China. The use of EXIM for funding could support the development, deployment, and management of secure, reliable 5G communications infrastructure worldwide and encourage international cooperation with our closest allies and cooperative nations. Unfortunately, this approach is hindered by EXIM's outdated U.S. content rules and does not readily apply to today's technology industry.

The current EXIM policy requires 85% U.S. content to get full EXIM financing. This is a difficult threshold for the technology industry to meet. The Chamber recommends that EXIM adopt a more flexible approach to U.S. content rules that may include considering U.S. R&D and intellectual property, as well as significantly lowering U.S. content requirements to support the national security priority to finance deployment of secure and trusted telecommunications infrastructure. EXIM will not be able to meet its statutory requirements under the Program on China and Transformation Exports unless it can provide export credit financing for 5G telecommunications transactions.

(5) Both the Department of Commerce and the Federal Communications Commission (FCC) have rulemakings underway to address the security of the telecommunications infrastructure supply chain. Are there other models that identify and manage risks that might be valuable to consider?

Addressed in other line of efforts.

(6) What other actions should the U.S. Government take to fulfill the policy goals outlined in the Act and the Strategy?

In addition to the recommendations discussed, the administration should work with Congress to pass the following legislation:

- Enact the Multilateral Telecom Security Fund Intelligence Authorization Act for Fiscal Year 2021 (S. 3905). This legislation establishes a $750 million fund jointly administered by the Office of the Director of National Intelligence and the Department of Defense, with the funds available for 10 years to help encourage the adoption of "trusted and secure equipment" worldwide.
- The administration should work with Congress to make clear that it is the policy of the U.S. government that our economic and national security interests are advanced by helping foreign governments invest in secure and trusted 5G telecom infrastructure. The administration worked with Congress on a similar precedent outside of the telecommunications market, the European Energy Security and Diversification Act of 2019 (P.L. 116-94, Div. P, Title XX) and this legislation could serve as model for a similar statement regarding 5G infrastructure.
- The administration should also work with Congress on new legislation to ease requirements for secure and trusted 5G telecom infrastructure projects in foreign markets.