CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

VINCENT M. VOCI
EXECUTIVE DIRECTOR, POLICY AND OPERATIONS
CYBER, INTELLIGENCE, AND SUPPLY CHAIN
SECURITY DIVISION

ABEL TORRES
SENIOR DIRECTOR
CENTER FOR GLOBAL REGULATORY COOPERATION

April 28, 2021

Jaclyn Rosen
Mobility Division
Wireless Telecommunications Bureau
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Mary Claire York
Mobility Division
Wireless Telecommunications Bureau
Federal Communications Commission
45 L Street, NE
Washington, DC 20554

Re: Promoting the Deployment of 5G Open Radio Access Networks, GN Docket No. 21-63; 86 FR 16349

Dear Ms. Rosen and Ms. York:

On behalf of the U.S. Chamber of Commerce, we are pleased to provide these comments to the Federal Communication Commissions Notice of Inquiry on promoting the deployment of 5G Open Radio Access Networks – GN Docket No. 21-63.

We believe that fifth-generation 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 in the next decade and beyond. The promise of 5G only will be fully realized globally 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, ensures robust deployment, adopts secure networks, and manages the risks to our economic and national security. Open Radio Access Networks (Open RAN) are an important part of this strategy and are in the early stages of maturation. Accordingly, the significant potential of Open RAN to drive solutions for 5G, and future telecommunications networks, will take time before users can fully realize them.

Accordingly, the Chamber urges the U.S. government to take the following actions:

1. Facilitate technology-neutral policies, which support open, interoperable, and virtualized solutions.
2. Accelerate deployment of all 5G technologies and use cases.

3. Support investments in innovation and research and development (R&D), with a focus on foundational next-generation (*i.e.*, 6G) research and development (R&D).
4. Uphold fair processes in standards-setting bodies.
5. Provide strong intellectual property rights for innovators.
6. Help allies see a larger market for trusted vendors.

The Chamber is fully supportive of the successful, trusted, and secure deployment of 5G communications systems and networks in the U.S. and abroad. Fiber-enabled 5G networks will be the most advanced and secure system deployed to date, with faster speeds, higher bandwidth, and lower latency. As a result, 5G networks have the potential to enable and support a wide range of applications (*e.g.*, autonomous vehicles, remote surgery, virtual reality, the Internet of Things, and others), far beyond what current networks can support. The private sector is currently deploying these networks and is developing procedures to identify, manage, and mitigate risks from the novel application of next-generation technologies.

Governments worldwide continue to orient themselves to deal with myriad issues associated with the deployment of this cutting-edge technology, to include: the availability and integrity of networks; the security and resilience of the supply chains that support them; and the confidentiality and privacy of data that flows over, through, and is stored on, such networks. 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 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. Governments also should support the continued development of trusted 5G technologies, services, and products by small and large vendors and new market entrants.

Tech Neutral, No Government Mandates

As previously noted, industry is leading the innovation and deployment of 5G technologies and solutions. The private sector is in the best position to develop and deploy the most appropriate and suitable technology to meet their customers' needs and mission requirements—including those of government customers—connected with the development, acquisition, use, and commercialization of 5G. From the perspective of Open RAN technology development, any policies or regulatory actions taken by the FCC or any federal agencies should (a) not unduly discriminate between technologies; or (b) mandate or prescribe by regulation or government contract use of specific technologies or specifications. Either of which action could negatively impact current RAN vendors, negatively impact the pace of secure and trusted 5G deployments in the U.S., and artificially impact the ecosystem in a manner inconsistent with traditional market-based concepts.

We believe that the federal government should not choose winners and losers in the open market. Accordingly, the Chamber opposes mandating Open RAN as a requirement in any of FCC's proceedings, including Universal Service Fund disbursements. The Chamber appreciates the FCC's determination that Open RAN solutions will be eligible for the Secure and Trusted Communications Network Reimbursement Program but should avoid mandating Open RAN solutions as a qualification for eligibility in future contract requirements. Our view is that deployment of enterprise 5G capabilities (*e.g.*, smart manufacturing, intelligent warehousing) will offer the most significant tangible value to customers at the earliest possible time.

The Chamber has historically supported policies that are "technology-neutral" in the sense that technologies and providers compete based on functions, capabilities, and requirements. Through this lens, we view the deployment of 5G architecture. We consider Open RAN as part of a longer-term solution, as demonstrated by the ongoing work within the O-RAN Alliance on open specifications. We support the development of secure open interfaces over time but not artificially accelerated by prescriptive regulation. The latter approach can force negative impacts on the marketplace, as outlined above.

Cybersecurity

Cybersecurity threats are evolving rapidly and are increasing in scale, frequency, complexity, and consequence. As 5G networks are deployed and utilized, it is essential to emphasize the security of those connections, devices, and applications. Enhanced security and resilience can be accomplished by aligning government policies to industry-vetted actions that businesses can take to assess and improve their security state over time. Allowing operators, equipment manufacturers, and vendors to combat evolving cyber threats with evolving best practices and standards permits a more flexible, current, and risk-based cybersecurity approach. We recommend that the FCC review the work of the Communications Security, Reliability, and Interoperability Council (CSRIC) VI and VII. CSRIC VIII could investigate 5G security standards, leveraging the work at 3rd Generation Partnership Project (3GPP) System Aspects (SA) Working Group 3. SA Working Group 3 is responsible for determining security and privacy requirements and specifying the security architectures and protocols.

Open architectures, such as those developed for Open RAN applications, can allow the operator to fully control the network's security, ultimately enhancing its security. Similarly, network operators will have greater visibility into security events and bring relevant security and resiliency expertise to the open architecture environment.

Additionally, operators of open architectures can build upon the capabilities enabled by 5G to shift the security capabilities closer to the edge of the network and identify and respond to attacks closer to the source. The introduction of open interfaces in the RAN allows the operator to distribute security analytics throughout the network and move security monitoring to the edge, with all the benefits, such as lower costs associated with the storage and transmission of data and better security and privacy leveraging edge-focused analytics As an example, an autonomous vehicle using edge computing sends data to a nearby access point where it is analyzed and returned, avoiding additional network hops it takes to send information to a centralized data center. Analysis at the edge will allow for quick identification of cybersecurity threats and the rapid resolution of security-related incidents. However, this is also possible in conventional RAN through definable parameters. The granularity of the data would be at a single base station.

Finally, the Chamber believes that more cybersecurity testing needs to be done on Open RAN stacks through groups such as CSRIC and the Open RAN Alliance. Open networks can accelerate the transition to complete network management automation. Automation enables zero-touch management, eliminating human intervention and the security risks inherent in human access to network functions (NF). In this context, zero-touch management means that automated networks will be capable of self-configuration, self-monitoring, self-healing, and self-optimization without any human intervention. This will reduce risks such as the threat of humans accidentally altering the security posture of a network function or maliciously harvesting credentials, changing configurations, or implanting malware within the network. That said, conventional RAN systems also offer zero-touch management through definable RAN parameters.

Global supply chain resilience and fostering market diversity

Supply chain security and resilience are fundamental to both the economic and national security of the U.S. and our allies. Over the past several years, there has been a consolidation of telecommunications equipment vendors, coupled with a significant rise in market share and penetration by certain high-risk vendors. Promoting secure and trusted supply chains, regardless of the generation of technology, is of global interest and will require a common solution. Governments should foster mandate-free policies where vendors are incentivized towards openness, interoperability, and virtualization.

There is a benefit and policy need for a more diverse set of secure and trusted suppliers for telecommunication equipment globally. Open RAN is a part of a larger strategy that drives increased competition, innovation, and network vendor diversity. Open interfaces and network infrastructure interoperable lowers barriers to entry and allows more market competition. This is not an immediate occurrence but will happen in the coming years as the technology is developed and deployed.

The Chamber has heard from its members that customer requirements increasingly drive the contours of future network design and architectures. Market-driven considerations for Open RAN stacks include:

1. Is there a degradation in performance (*i.e.*, latency, download speeds, power usage)?
2. Can the integrated stack manage security threats?
3. Can an Open RAN stack offer similar features and capability?

As the Chamber underscored in its recent letter on the risks in the semiconductor manufacturing and advanced packaging supply chain in response to the U.S. Department of Commerce's request for comments, semiconductors represent one of the most important industries to the U.S. economy. Semiconductors provide the foundation for a wide array of products and services. They enable advancements in artificial intelligence (AI), high-performance computing (HPC), 5G, Wi-Fi, Open RAN, and autonomous systems. Importantly, they power the digital infrastructure needed for remote learning, telehealth, and work-from-home. It is essential to acknowledge the role of semiconductor technology in the hardware for the Open RAN ecosystem. Semiconductors are central computing and processing hubs of the stack and are critical in the security and research and development supply chain. Innovation from semiconductors to the radio access network to the network edge is happening across the supply chain.

International cooperation

U.S. policy should expressly advance a diverse, trusted market of suppliers based in the U.S., allies, and other partner market democracies. Only a multinational, diverse vendor base of trusted suppliers will have the capacity to service the U.S. and other partner countries' markets. We encourage further international cooperation on security, standards, research and development, and innovation in telecommunications networks. We believe that there is growing consensus with allied governments on telecommunications security policy. However, more work needs to be done. We caution governments against supporting policies that champion local or domestic providers, manufacturers, and services. The Chamber believes that the current supply chain for ICT equipment, products, and services is global and supported by treaty-allied governments and international partners. If our goal is to promote trusted supply chain partners from across the globe, we need to be working with them to implement short-term solutions. The goal is to reduce reliance on high-risk vendors in the telecom marketplace. We more quickly achieve that objective by supporting the existing market but encouraging innovation and R&D in the next generation.

The Chamber supports *The Prague Proposals* endorsed at the 2019 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 provide design, construction, and administration recommendations for 5G infrastructure. The Prague Proposals emphasize the need for 5G networks to be built based on free and fair competition, transparency, and the rule of law. We welcome the international collaboration embodied in the process that led to the initial Proposals and look forward to future engagement.

The Chamber also recognizes the past leadership of the U.S. National Security Council, the U.S. Department of State, the U.S. Department of Commerce, and the Cybersecurity and Infrastructure Security Agency in working with allied governments 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*, including technical consultations with the U.S. government. We recognize the U.S. government for its international engagement and leadership and look forward to future opportunities for public-private collaboration.

Research and Development

The U.S. government should ensure that 5G networks are resilient against threats to their availability and integrity while protecting the confidentiality of the network. The Chamber supports federally-funded 5G innovation testbeds to enhance the performance, cybersecurity, and features of integrated 5G stacks and also supports additional testing be leveraged for national and homeland security purposes. R&D funding in 5G could accelerate trusted suppliers' development of the remaining capabilities around which there is so much interest, including end-to-end secure network slicing and dynamic spectrum sharing. And critically, funding could also help accelerate the development of use cases that will drive enterprise-level adoption of 5G, while ensuring that technologies, such as Open RAN, can scale with similar or new features and capabilities.

The development of innovation testbeds will accelerate application and use case development and progress the common interface specifications to enable an open ecosystem. This is essential to incentivize the adoption of 5G by individual enterprises and vertical industry segments. These initiatives would demonstrate progress and help industry and government test new solutions and invest in foundational research for critical new 6G technologies. By defining the desired end state and letting the industry innovate to that outcome, government agencies will spur a research and development cycle to position the U.S. as a global market leader in 5G technologies.

Financing

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. Further liberalizing EXIM financing and U.S. content restrictions 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.

The Chamber views EXIM as an essential tool at the disposal of U.S. companies to level the playing field for trade finance as they seek to increase exports and create American jobs. The recent domestic content reforms proposed by EXIM requiring 51% U.S. content, down from 85%, to qualify for EXIM financing has undoubtedly helped U.S. firms in these transformational industries to be able to compete on the global stage. The Chamber recommends that EXIM continue to adopt a more flexible approach to U.S. content rules that may include considering U.S. R&D and intellectual property and lowering U.S. content requirements to support the national security priority to finance the deployment of secure and trusted telecommunications infrastructure. EXIM will not meet its statutory requirements under the Program on China and Transformation Exports unless it can provide export credit financing for 5G telecommunications transactions. The Chamber looks forward to providing this feedback directly to EXIM through their Request for Comment on China and Transformational Exports Program.

The Chamber further urges the U.S. government to consider:

- Modernize the U.S. International Development Finance Corporation tools to enable better private capital mobilization to support 5G deployment and 5G-enabling digital infrastructures.
- Fully fund the USA Telcom Act, including the Multilateral Telecommunications Security Fund and Public Wireless R & D Fund.

As the U.S. government develops its implementation plan and considers new initiatives, the Chamber urges the U.S. government to continue leveraging the multi-stakeholder process underpinning 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.

Conclusion

Thank you for the opportunity to comment on the FCC's Notice of Inquiry on this issue. We look forward to working with you and your colleagues at the Commission on the domestic and global deployment of next-generation secure and trusted information and communication technologies and networks.

Sincerely,

Vincent Voci

Abel Torres