Before the
U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G Implementation Plan	)	Docket No. 200521-0144
	)	RIN 0660-XC047
	)	

COMMENTS OF
USTELECOM – THE BROADBAND ASSOCIATION

USTelecom[1] is pleased to submit these comments in response to the National Telecommunications and Information Administration's ("NTIA") Request for Public Comments ("RFC"), which seeks to inform the development of an Implementation Plan for the National Strategy to Secure 5G.[2]

This proceeding comes at an important time. Not only are we at a critical crossroads in determining how government and industry will tackle the challenges posed by 5G deployment and the threats posed by increasing national security risks, but industry also is in the process of working through the impacts of COVID-19, which has placed unprecedented demands on the communications networks that enable connectivity and remote work and learning. The pandemic has reinforced the need for a coordinated national communications policy to provide secure and reliable connectivity for first responders, educational institutions and students,

[1] USTelecom is the premier trade association representing service providers and suppliers for the communications industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse membership ranges from international publicly traded corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country.

[2] National Telecommunications and Information Administration, *The National Strategy to Secure 5G Implementation Plan*, Notice, Request for Public Comments, Docket No. 200521–0144, 85 FR 32016 (May 28, 2020) ("RFC").

commerce, telehealth, and other underserved aspects of society. USTelecom and its members are committed to being part of the solution to all of these inter-related challenges.

In that spirit, USTelecom offers its perspective on key issues raised by the RFC. As discussed below, the strategy for secure 5G must include meaningful steps toward eliminating barriers to deploying the fiber that will be essential to supporting 5G networks. In addition, the strategy should recognize that the future of secure 5G connectivity will require public-private collaboration on security measures, a supply chain consisting of trusted and allied suppliers, and a diverse and global vendor base – all of which the U.S. government is in a position to promote.

DISCUSSION

I. THE IMPLEMENTATION PLAN FOR THE NATIONAL STRATEGY TO SECURE 5G MUST ACCOUNT FOR THE CRITICAL ROLE PLAYED BY WIRELINE NETWORKS AND FACILITATE THE DEPLOYMENT OF FIBER

USTelecom fills an important gap in the 5G policy discourse, as its members are leaders in both wireless and wireline technologies. As such, we can expertly vouch for the fact that a secure 5G strategy cannot be focused on 5G spectrum alone. While enlightened spectrum policy is certainly necessary for successful 5G deployment, it is only one piece of the puzzle. Fiber backhaul facilities are just as important.

Simply put, fiber optic networks will play a prominent role in enabling 5G infrastructure. Once fiber is in place, it can easily scale to accommodate higher speeds and expected growth in capacity demands. Thus, fiber will necessarily be deployed broadly throughout emerging 5G networks as an essential component in implementing 5G capabilities and capacities. Fiber also will enable the secure transmission of enormous quantities of data, via wireline fronthaul and backhaul facilities, as consumers, businesses including IoT, and manufacturing become more fully connected.

As part of its 5G spectrum strategy, the U.S. government therefore should take steps to streamline the deployment of fiber facilities necessary for 5G.[3] At present, numerous impediments to that deployment remain, which USTelecom and others have documented extensively in other governmental arenas and proceedings.[4] These obstacles include, but are not limited to, unreasonable zoning, permitting, power, construction moratoriums, and aesthetic restrictions on antenna placement. We recommend that the Administration focus on removing these barriers in implementing the National Strategy to Secure 5G. Doing so will ensure competitive positioning and thereby increased resiliency of U.S. wireless networks and accelerate customer adoption of the virtually limitless applications that will be enabled by this new generation of 5G wireless services.

II. CONTINUED PUBLIC-PRIVATE COLLABORATION IS ESSENTIAL TO THE FUTURE OF SECURE CONNECTIVITY

As the Administration is well aware, both industry and various governmental actors are taking active steps to address supply chain security and 5G security in particular. USTelecom is an active participant in all of those efforts. Of note, among its leadership roles, USTelecom founded and presently co-leads with the Consumer Technology Association the Council to Secure the Digital Economy ("CSDE"), a group of over a dozen large international information and communications technology ("ICT") companies dedicated to preserving the security of our communications infrastructure and connected digital ecosystem. CSDE has been recognized by this Administration as a leading industry partnership in coordinating efforts to combat botnets,[5]

[3] RFC at 32,017, Line of Effort One (asking how the U.S. government can best facilitate the domestic rollout of 5G technologies).

[4] *See generally, e.g.*, Comments of USTelecom – The Broadband Association, Docket No. 191119-0084 (Dep't of Commerce filed Jan. 10, 2020).

[5] CSDE, *International Botnet and IoT Security Guide 2020*, https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf; *see also* U.S. Department of Homeland Security

respond to cyber crises,[6] and promote IoT security[7] – all of which will be of increasing importance as we work to build a secure 5G ecosystem. Meanwhile, various government initiatives regarding network and device security are ongoing within the interagency, with the National Institute for Security and Technology ("NIST") and the Departments of Defense, Homeland Security, and Commerce all conducting different parallel processes, among others. In those settings, USTelecom and many others have consistently called for a well-coordinated whole-of-government approach that ensures consistency among all of these efforts.

In considering what specific security measures belong in its plan to implement the National Strategy to Secure5G, the Administration should strategically coordinate these efforts and ensure that the implementation plan leverages all of them together, rather than diverging from them or allowing these efforts to splinter from each other. USTelecom's members fully expect to embrace and follow reasonable security measures necessary to protect 5G networks. We simply ask for proper coordination on security policy and related initiatives to avoid undue costs and delays on 5G network deployments, which will adversely affect network providers' ability to effectively deploy network assets to meet demand.

In particular, USTelecom would like to better understand the scope and impact of any potential security measures and to have an opportunity to collaborate on any new measures proposed to avoid conflicts that could undermine deployment efforts. For instance, in reference

& U.S. Department of Commerce, *A Road Map Toward Resilience Against Botnets* (Nov. 29, 2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf (listing CSDE as a contributor for a variety of tasks in 2019-2020, including "Defining a Core Security Capability Baseline").

[6] CSDE, *Cyber Crisis: Foundations of Multi-Stakeholder Coordination* (Sept. 2019), https://www.ustelecom.org/wp-content/uploads/2019/09/CSDE-Report-Cyber-Crisis-Foundations-of-Multi-Stakeholder-Coordination.pdf.

[7] CSDE, *The C2 Consensus on IoT Device Security Baseline Capabilities* (Sept. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

to "Line of Effort Two,"[8] we should not look past the existing security control regime as specified in NIST 800-171, which allows companies to have a standard reference to provide security controls regarding Controlled Unclassified Information ("CUI") to their customers. NIST 800-171 is also the basis of the new Cybersecurity Maturity Model Certification ("CMMC") program currently being implemented by the Department of Defense as part of a program to better secure the supply chain for hardware and software used by suppliers of services to the DoD. The Administration's implementation plan should allow network service providers to follow NIST 800-171 and the CMMC standards for network providers' federal customers, and, more generally in all cases, promote use of the NIST Cybersecurity Framework – particularly the groundbreaking implementation recommendations for communications providers developed under USTelecom's leadership by the Communications Security, Reliability, and Interoperability Council ("CSRIC").[9] Such an approach will leverage the significant effort already expended by the communications sector, NIST, and the Defense Department, and avoid the sort of overlapping or conflicting security regimes that risk impeding 5G deployment.

III. SECURING THE 5G ECOSYSTEM REQUIRES THE DEVELOPMENT OF A SUPPLY CHAIN CONSISTING OF BOTH TRUSTED AND GLOBAL VENDORS

Although the RFC understandably highlights actions that could be taken to create economic opportunities for U.S. companies,[10] the Administration should not focus on U.S. companies alone as the solution for a secure 5G ecosystem. The ICT marketplace is global, and

[8] RFC at 32,017, Line of Effort Two: Assess Risks to and Identify Core Security Principals of 5G Infrastructure.

[9] CSRIC IV Working Group Four, *Final Report: Cybersecurity Risk Management and Best Practices* (Mar. 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.

[10] *Id.*, Line of Effort Three: Address Risks to U.S. Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

the trusted supply chain must be global as well – that is, it must include allied suppliers rather than using exclusively U.S.-based manufacturing as the only criteria of trust.

In working toward that outcome, the Administration need not start from scratch; rather, various efforts already underway can inform and advance the development of a global network of trusted suppliers. In particular, the National Strategy to Secure 5G should reflect and affirm the principles and goals of the "Prague Proposals for 5G," a set of recommendations aiming to promote a diversity of market participants in lieu of only few dominant players that can pose threats to national security. The Prague Proposals, which were developed by the United States and thirty-one other countries, are premised on the rule of law, independent judiciary, corporate transparency and accountability, and security by design. Several efforts are underway to further entrench these values in U.S. policymaking. Of note, the Center for Strategic and International Studies ("CSIS") organized a working group consisting of over two dozen industry experts to develop criteria for governments and network operators to use to implement the Prague Proposals and the European Union's 5G Toolbox to assess trustworthiness and security.[11] These criteria are intended to be practical, concrete criteria for governments and network operators to implementing the Prague Proposals and the European Union's 5G Toolbox to assess trustworthiness and security. In addition, House Resolution 575 would affirm the support of the United States for the Prague Proposals; by passing this resolution, the U.S. Senate would shore up the U.S. government's affirmation of these values.

The National Strategy to Secure 5G should also look to the formal industry-government collaboration taking place under the auspices of the Department of Homeland Security's

[11] *See* Center for Strategic and International Studies, *Criteria for Security and Trust in Telecommunications Networks and Services* (May 13, 2020), https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

Information and Communications Technology Supply Chain Risk Management Task Force for guidance on how suppliers can develop trusted relationships among themselves. USTelecom serves as one of three co-chairs of the Task Force, and various USTelecom members are playing lead roles in that process. For instance, CenturyLink is co-chairing a working group focused on mitigating legal risks associated with information sharing; meanwhile, Verizon and Samsung are leading a separate working group focused on the development of a security template. These collaborative activities between U.S. and non-U.S. headquartered companies illustrate the current global nature of the supply chain. The Administration's implementation plan should embrace that allied international approach to ensure a secure 5G ecosystem.

IV. A DIVERSE VENDOR BASE WILL GENERATE ECONOMIC AND SECURITY BENEFITS FOR THE U.S. AND THE SECURE 5G ECOSYSTEM

One of the most important things that the U.S. government can do to improve network equipment security and reliability is to promote policies that stimulate and maintain vendor diversity. More choice in the marketplace leads to better and more secure outcomes for buyers, as vendors in a competitive market will survive only by offering innovative, secure, and constantly improving products.

The RFC appears to accept this point as an underlying premise of the implementation plan, as it identifies "5G vendor diversity" as a goal and asks how it can best be achieved.[12] That acknowledgement is important, because the trend in the network equipment marketplace in the last two decades has been away from vendor diversity, offering less and less choice for network equipment purchasers. In particular, China has contributed to the lack of vendor diversity.

[12] *Id.*

It is widely acknowledged that certain Chinese government-backed companies currently threaten to squeeze the global communications network supply chain. Their ascent is no accident, and it presents economic security risks to the United States and other countries. Recognizing that technological dominance brings economic and geopolitical power, China more than a decade ago put into place a deliberate strategy for reaching its current marketplace heights. In 1994, China's wireless infrastructure was 100 percent imported.[13] By 2001, Chinese vendors held 77 percent market share in the country.[14] That trend repeated itself with 4G. Starting with a 48 percent share of the wireless infrastructure market in China in 2011, Chinese vendors held an 83 percent share in 2018.[15]

Support from the Chinese government underpins this dramatic expansion of market share – and squeezing of other suppliers – both in China itself and globally. Late last year, the *Wall Street Journal* detailed how Huawei got access to as much as $75 billion in state support as it grew into the world's largest communications equipment vendor.[16] To put this amount in perspective, the size of the entire global communications network equipment marketplace is about $76 billion annually. The FCC, as well, has noted that Huawei "is reported to benefit from vast subsidies from the Chinese government."[17] Huawei's skyrocketing revenues, well over $100 billion in 2019, allowed it to fund research and development, leading to innovations and

[13] *See* Evolution of China's Telecommunications Manufacturing Industry: Competition, Strategy and Government Policy, Zixiang Tan, Communications & Strategies no. 53, 1st quarter 2004, ad page 82, Table 3.

[14] *Id.* This includes subsidiaries and joint ventures of Chinese companies.

[15] IHS Markit, Mobile Infrastructure: China, Market Report, April 12, 2019. Source – Omdia, Mobile Infrastructure Market Report – China – 2020, China Market Share. Results are not an endorsement. Any reliance on these results is at the third-party's own risk.

[16] Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, Wall St. J., Dec. 25, 2019.

[17] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, 34 FCC Rcd 11423, 11443 (2019).

patents that give the company a further edge over the competition.[18] Meanwhile, Huawei's competitors, which do not enjoy anything close to the same level of government backing, experienced substantial market consolidation. By 2018, 96 percent of the RAN equipment market was accounted for by only five vendors – trusted vendors Ericsson, Nokia, and Samsung, plus the two Chinese vendors subject to U.S. government restrictions – as Lucent, Siemens, Nortel, Motorola, and Panasonic have all exited the RAN market.[19] During this same time, Huawei's share of the global wireless infrastructure market increased from zero in 2000 to 31 percent by 2018.[20]

That consolidation presents substantial risks to trusted vendors because the communications equipment market is characterized by economies of scale – and their ability to remain competitive would be harmed absent a level global playing field. The U.S. market by itself is not sufficient for equipment vendors to achieve sufficient economies of scale, so addressing the troubling trend towards consolidation requires coordinating policies with like-minded countries that promote economic security in the form of vendor diversity and a competitive marketplace.

While China has driven many of the current imbalances, other opportunities for imbalances in market equities are possible that will impact the nation's economic security. Accordingly, without some form of analysis to assure our sustained, economic security, we are

[18] Huawei reported annual revenues of $123 billion in 2019. Huawei Investment & Holding Co., Ltc., 2019 Annual Report, at 9, available at https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report_2019_en.pdf?la=en. In a June 2019 paper, Barclay reported that in the past year, Huawei had spent more on research and development than Ericsson and Nokia combined. *5G Leadership: Huawei in Context, Special Report*, June 5, 2019 at 18.

[19] *How Will 5G Shape Innovation and Security, A Primer*, James A. Lewis, Center for Strategic & International Studies, December 2018 at 4; Barclays, *5G Leadership, Huawei in Context, Special Report*, June 5, 2019 at 21.

[20] *How Will 5G Shape Innovation and Security, A Primer*, James A. Lewis, Center for Strategic & International Studies, December 2018 at 4 (chart of RAN Equipment market leaders, showing Huawei at 31%).

likely to repeat ourselves. With a plan, we are in a better position to sustain our nation's economic security and our nation's resilience. The plan, however, should not be for the U.S. to simply pick a national vendor and for the U.S. to place all of its emphasis behind it—this does nothing to further the types of vendor diversity that USTelecom believes necessary to create long-term economic security for 5G and beyond.

Loss of competitive options runs the risk of depressing the innovation needed to keep the U.S. and allied communications industry on the leading edge of technology. Moreover, such reduced choice would inherently implicate national security concerns, even with trustworthy vendors. Communications networks forced to rely on a narrow array of infrastructure options become increasingly vulnerable to "single point of failure" risks no matter who is the vendor. When the choice has been winnowed down to vendors that the government has found to be untrustworthy, the security situation is untenable.

While there are likely numerous actions that the U.S. government can take to promote 5G vendor diversity and foster market competition,[21] promotion of rigorous and consensus-based technical standards that allow for open interfaces and interoperability among network components is a necessary element of all such policies. To take one example, many USTelecom members are leading proponents of advancing open and interoperable RAN equipment that allows a more modular approach to network design and deployment, so that network operators need not be dependent on a single equipment vendor.[22] The ability to offer modular components lowers entry barriers for vendors, who can enter the market gradually. The more opportunity

[21] RFC at 32,017.

[22] USTelecom members are among the founders and leaders of the O-RAN Alliance and the Open RAN Policy Coalition, which, respectively, promote (1) open and interoperable technical standards in the RAN and (2) policies designed to advance this technology in real-world deployments. *See* https://www.o-ran.org/ and https://www.openranpolicy.org/.

there is to sell interoperable network components, the more vendors are encouraged to innovate, and the more options a provider can have in developing diverse network equipment solutions. All of this makes providers less dependent upon a sole-source product, such as Huawei equipment, that can harm national interests. The U.S. government should continue to promote open and interoperable network components in the RAN and throughout all elements of the wireless and wireline networks that will enable 5G.

CONCLUSION

USTelecom looks forward to working with NTIA and other key stakeholders in industry and the Administration to develop and implement policies that promote the deployment of secure and reliable 5G infrastructure and, in so doing, preserve the technological leadership of the United States.

Respectfully submitted,

Robert Mayer
Senior Vice President, Cybersecurity
USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

Michael Saperstein
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

June 25, 2020