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 VERIZON

William H. Johnson
Of Counsel

Gregory M. Romano
Christopher D. Oatway
Tamara L. Preiss
VERIZON
1300 I Street, NW
Suite 500 East
Washington, DC 20005
(202) 515-2400

Counsel for Verizon

June 25, 2020

TABLE OF CONTENTS

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	)	Docket No. 200521-0144
Implementation Plan	)	RIN 0660-XC047
	)	
	)	

COMMENTS OF VERIZON

As we noted at the time, the Administration's call last year for a comprehensive spectrum strategy was both timely and necessary.[1] We called for policies to help facilitate a successful 5G revolution and cement the United States' position as a wireless leader for generations to come. More than a year later, much work has been done, and much remains. We welcome the opportunity to provide input to inform the development of an Implementation Plan for the National Strategy to Secure 5G.[2] U.S. consumers, workers, and the U.S. economy will benefit from tremendous innovation and capital investment if the Administration seizes the opportunity to implement policies that promote robust 5G deployment of equipment manufactured by a trusted bench of competitive vendors.

---

[1] Comments of Verizon, Docket No. 181130999-8999-01, RIN 0660-XC044, at 1 (filed Jan. 22, 2019).

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

Because spectrum – especially mid-band spectrum – is critical to successful 5G deployment, it is crucial that the Administration work with the Federal Communications Commission ("FCC") to repurpose and license additional spectrum. Also important to promoting the United States' 5G competitiveness are policies that continue to remove roadblocks to deploying 5G infrastructure, so that Verizon and other service providers can efficiently and effectively spend the tens of billions of dollars on capital investment to which we have committed. The Administration also should view cybersecurity as a market differentiator, which means abandoning "lowest price technically acceptable" procurement policies and working with industry on cutting-edge security opportunities such as "Zero Trust Architecture." And economic security should be the centerpiece of the Administration's domestic and foreign policies: the Administration, in conjunction with like-minded countries around the globe, should help ensure that service providers both in the United States and abroad will continue to have a robust, competitive bench of trusted vendors.

I. WIDESPREAD AND SUCCESSFUL 5G DEPLOYMENT DEPENDS ON ACCESS TO LARGE SWATHS OF SPECTRUM AND SMART POLICIES THAT FOSTER NEXT-GENERATION INFRASTRUCTURE BUILDS

A. Spectrum – Especially Mid-Band Spectrum – Is Critical to the Deployment of Robust 5G Networks.

Verizon is the leader in 5G, building the most powerful 5G experience across the nation. We were first to deploy 5G in the United States in 2018, with our 5G Home internet service in parts of multiple cities.[3] And our 5G Ultra Wideband mobile service delivers ultra-fast speeds that are ten times faster than some other 5G networks.[4] It also provides massive network

[3] *See* Verizon, *When will Verizon have 5G?* (Dec. 5, 2019), https://www.verizon.com/about/our-company/5g/when-will-verizon-have-5g.

[4] Verizon, *There's 5G. Then there's Verizon 5G*, https://www.verizon.com/5g/ (last visited June 8, 2020).

capacity to support millions of connections, greatly reduces latency, and will fundamentally change the way we live, learn, work, and play. By focusing on public spaces, downtown areas, and stadiums and arenas (we are in 17 National Football League stadiums and seven arenas),[5] we have targeted the areas that will benefit the largest number of people in our early stages of mobile deployment. We deploy our 5G Ultra Wideband mobile service using millimeter wave ("mmW") spectrum as a cornerstone in 35 cities across the country.[6] We are using a new technology, Dynamic Spectrum Sharing ("DSS"), in our low- and mid-band spectrum to allow us to leverage our spectrum to provide both 4G and 5G service. DSS allows us to use our spectrum more efficiently than ever before as the nation makes the transition from 4G to 5G networks.

As the Administration and the FCC are well aware, however, large, contiguous blocks of mid-band spectrum, made available for licensed, flexible-use service, will be critical for U.S. leadership in 5G. Over the past two years, the FCC has made extraordinary progress in unleashing new sources of spectrum for 5G. As part of its 5G FAST Plan,[7] the FCC has auctioned almost 5 gigahertz of high-band spectrum in the 24, 28, 37, 39, and 47 GHz bands.[8] Prior to that, the FCC repurposed low-band 600 MHz spectrum for flexible-use and 5G in the broadcast incentive auction.[9] Most important, the FCC has worked to address the dearth of licensed mid-band spectrum for 5G in the United States, including with its order to repurpose

[5] Verizon, *5G Mobile FAQs*, https://www.verizonwireless.com/support/5g-mobile-faqs/ (last visited June 8, 2020).

[6] Verizon, *Explore Verizon 5G Ultra Wideband coverage*, https://www.verizon.com/5g/coverage-map/ (last visited June 8, 2020).

[7] FCC, *The FCC's 5G FAST Plan*, https://www.fcc.gov/5G (last visited June 8, 2020).

[8] *Id.*

[9] *Id.*

280 megahertz of spectrum in the 3.7-3.98 GHz C-band for 5G use that will enable wide-band channelization.[10]

Despite this progress, additional mid-band spectrum will be needed to enable 5G coverage and capacity, so it is critical for the Administration and NTIA in particular to work closely with the FCC to repurpose and license as much additional mid-band spectrum as possible. In particular, we urge the government to move forward on repurposing the lower 3 GHz band.[11] Such spectrum should be made available in large, contiguous blocks to allow for improved efficiency, and technical rules should enable large-scale 5G deployments. Overly strict emission limits or power levels could unnecessarily constrain operations and reduce the coverage that can be provided.

B. Smart 5G-Friendly Infrastructure Policies are Equally Important to the Deployment of 5G.

Policymakers also must commit to 5G-friendly infrastructure policy. Too often, federal, state, and local authorities erect burdensome roadblocks to the deployment of spectrum. The FCC and the Administration have taken significant steps in recent years to remove those obstacles,[12] but more work remains.

---

[10] *Expanding Flexible Use of the 3.7 to 4.2 GHz Band*, GN Docket No. 18-122, Report and Order and Order of Proposed Modification, 35 FCC Rcd 2343 (2020).

[11] *See, e.g.*, NTIA Technical Report TR-20-546, *Technical Feasibility of Sharing Federal Spectrum with Future Commercial Operations in the 3450-3550 MHz Band*, Jan. 2020, https://www.ntia.doc.gov/files/ntia/publications/1-24-2020_ntia_tr-20-546.pdf; Charles Cooper, Associate Administrator of the Office of Spectrum Management, NTIA, *NTIA Report Finds Viable Options for Spectrum Sharing in 3450-3550 MHz Band*, Jan. 27, 2020, https://www.ntia.doc.gov/blog/2020/ntia-report-finds-viable-options-spectrum-sharing-3450-3550-mhz-band (noting that NTIA will report later this year on a further study of the 3100-3550 MHz band).

[12] *See, e.g.*, *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*, WT Docket No. 17-79, Second Report and Order, 33 FCC Rcd 3102 (2018) (streamlining tribal reviews of wireless deployment), *aff'd in part and rev'd in part*,

First, technology-agnostic rules will help encourage 5G deployment. Federal regulations that govern infrastructure siting reflect yesterday's voice-centric networks and are not tailored for today's data-driven economy and the broadband networks that support it. Policies designed to promote broadband generally and 5G networks in particular should not be premised on a legal framework that turns on distinctions between voice and data networks.[13] Congress and the Administration should review that framework, eliminate outmoded distinctions, and enact laws and policies that affirmatively promote the deployment of broadband infrastructure.

Second, Congress should amend Section 332(c)(7) to make clear that otherwise legitimate state and local interests in reviewing and approving the placement of broadband facilities must not undermine the compelling federal interest in promoting the deployment of broadband infrastructure. Congress should adopt shot clocks on state and local reviews of siting applications, enforced by "deemed granted" remedies in the event that states or localities do not act before the shot clocks expire. It should mandate cost-based rates for access to rights-of-way or to attach to structures within the rights-of-way, and make clear that states and localities may not discriminate in granting that access.[14] To the extent that localities impose aesthetic requirements as part of the siting process, Congress should require that they be reasonable, non-discriminatory, and disclosed in advance.

United Keetoowah Band of Cherokee Indians v. FCC, 933 F.3d 728 (D.C. Cir. 2019); *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*, WT Docket No. 17-79, WC Docket No. 17-84, Declaratory Ruling and Third Report and Order, 33 FCC Rcd 9088 (2018) ("*Small Cell Order*"), pets. for review pending, *Sprint Corp. v. FCC* (9th Cir.); Executive Order 13821, *Streamlining and Expediting Requests to Locate Broadband Facilities in Rural America*, 83 Fed. Reg. 1507 (Jan. 11, 2018); *Updates to the Regulations Implementing the Procedural Provisions of the National Environmental Policy Act*, Notice of Proposed Rulemaking, 85 Fed. Reg. 1684 (Jan. 10, 2020).

[13] *See, e.g.*, 47 U.S.C. §§ 253, 332, 1455(a).

[14] *See, e.g.*, *Small Cell Order*, 33 FCC Rcd 9088 (2018).

Finally, Congress, the Administration, and the FCC should work together to eliminate costly, dilatory, and unnecessary environmental and historic preservation reviews of certain wireless infrastructure. Too often, 5G infrastructure deployment is delayed by regulatory approval processes that almost never result in any findings of harm. Small wireless facilities are typically deployed in rights-of-way either on existing structures – like utility poles and street lights – or on new poles designed to blend with the environment. These poles pose no threat to the environment because the area around them has been developed, and any effects to historic properties can be eliminated by reasonable design criteria and by placing new poles on previously developed ground (such as rights-of-way). Recently, the President issued an Executive Order requiring the executive agencies to take steps to eliminate environmental barriers to infrastructure deployment.[15] In furtherance of that order, Congress and the U.S. government generally should eliminate environmental and historic preservation reviews of certain small wireless facilities.[16]

II. THE U.S. GOVERNMENT SHOULD LEVERAGE PRIVATE SECTOR ADVANCES TO PROMOTE ROBUST 5G SECURITY PRACTICES

A. Security Drives Verizon's Design and Operation of Its 5G Network.

The advent of 5G communications will provide dramatic increases in both bandwidth and upload/download speeds, and extraordinary decreases in latency. Together, these improvements will not only expand technical capabilities but also drive exponential increases in the number of connected devices in every sector of the economy. The 5G revolution will thus also expand the "attack surface" for cyber threats, including sabotage and espionage by sophisticated actors, both

[15] Executive Order 13927, *Accelerating the Nation's Economic Recovery from the COVID-19 Emergency by Expediting Infrastructure Investments and Other Activities*, 85 Fed. Reg. 35165 (June 9, 2020).

[16] *See, e.g.*, 47 C.F.R. § 1.6002(l) (defining small wireless facilities).

through the convergence of the cyber and physical worlds and through the massive increase in all types of digital data. Technological advancements throughout history have created opportunities for both good and bad actors, and there is no doubt that criminals, spies, and saboteurs will seek to leverage 5G to their malicious ends.

Verizon designs and deploys its 5G network with full awareness of these threats, and we operate and improve the security functions of our network in a manner that accounts for them. In short, security drives how Verizon builds and operates its 5G network. Our goal is to make sure every element of our 5G network implements security controls that deliver confidentiality, integrity, and availability, so that the overall network provides subscribers with a secure communications channel, and so that security is yet another factor that makes our wireless network best in class. Verizon's approach to securing our 5G network rests on four pillars:[17]

1. **Leveraging Verizon's Leading Global Security Capabilities.** The first pillar of Verizon's approach to securing our 5G network is leveraging our existing leading global security capabilities, including: (1) physical security of our facilities, penetration testing of key systems, an enterprise vulnerability management program, global security operations centers, supply chain security practices relying on trusted vendors that have undergone our rigorous vetting processes, and best-in-class security governance programs; (2) partnerships with industry groups such as such as the Communications Information Sharing and Analysis Center ("Comm ISAC"), the FCC's Communications Security, Reliability, and Interoperability Council ("CSRIC"), the Alliance for Telecommunications Industry Solutions ("ATIS"), and the Department of Homeland Security's ("DHS") Information and Communications Technology ("ICT") Supply Chain Risk Management ("SCRM") Task Force; and (3) a global backbone network providing visibility into worldwide threats that Verizon uses to inform the defense of its networks.

2. **Deploying Security Features from 5G Standards.** The second pillar of Verizon's approach to securing our 5G network is leveraging new security features that are part of the 3rd Generation Partnership Project ("3GPP") 5G technical standards, which we ourselves have helped develop, to provide new security features that did not exist in

[17] *See generally* Verizon White Paper, "First Principles for Securing 5G: The Design, Deployment, Operation, and Innovation of Secure 5G Networks" (Dec. 2019), *available at* https://enterprise.verizon.com/resources/biz/whitepapers/first-principles-for-securing-5G-white-paper.pdf.

previous generations of wireless technology. Verizon's 5G network will implement numerous such features to enhance security, and 3GPP's new trust model and security architecture have informed our implementation decisions. These include: (1) user equipment security features include protecting information that could be used to identify and track a subscriber, preventing attackers from modifying user traffic, and ensuring subscribers only connect to trusted cell sites; (2) Radio Access Network ("RAN") security features provide secure communications on all RAN interfaces and include extra protections at places that are vulnerable to physical attacks; and (3) Core Network security features include specialized network functions and enhanced protections for the new Service-Based Architecture ("SBA") that network functions will use to communicate.

3. **Enhancing Security via Features Unique to Verizon's 5G Implementation.** The third pillar of Verizon's approach to securing our 5G network is enhancing security by building in unique features. We routinely assess the software and hardware that goes into our network, and we employ rigorous, documented policies and procedures for secure configuration and operation of equipment and devices we deploy throughout the network. We take advantage of flexibility in 5G standards to design, implement, and deploy our network with this heightened security posture. Verizon's unique security features include: (1) design decisions built on Verizon's robust 4G LTE security principles as well as tailoring redundancy models and security features for each network function; (2) implementation that provides a robust device certification process, hardening key infrastructure services and network interfaces, and securely provisioning and booting network functions; and (3) deployment capabilities to utilize core services such as Public Key Infrastructure, access management, security analytics, vulnerability scanning, and software scanning.

4. **Enabling Advanced Customer-Facing Security Services.** The fourth pillar of Verizon's approach to securing our 5G network is using 5G's new capabilities to enable new customer-facing security services. 5G provides unprecedented flexibility and agility to create services on demand at locations throughout the network. We will leverage this to offer customers new services that were otherwise not possible. These capabilities include: (1) "network slicing," which provides various levels of isolation and resource guarantees to customers' service needs; (2) orchestration that dynamically instantiates security services for customer applications and devices; and (3) Multi-Access Edge Computing ("MEC"), which will host latency-sensitive, network-based security services that are tailored for customer applications and devices.

These four pillars and their associated features for 5G build upon 4G security, improve it in key areas, and provide an overall higher level of security in 5G than in 4G LTE. Verizon's 5G implementation builds additional capabilities to make our 5G security a differentiator in the

marketplace. Combined, these characteristics make Verizon's 5G network more secure than what was possible under 4G LTE and previous generations.

B. U.S. Government 5G Initiatives and Procurement Authority Should Advance Specialized Security Capabilities.

Based on this foundation of security-oriented innovation in the design and operation of Verizon's own 5G network, we urge policymakers to appreciate that depending on the care, expertise, and technical rigor with which a 5G network is deployed – particularly in the early deployment of 5G – such networks can vary widely in their capabilities and security. We thus recommend that the U.S. government orient its 5G initiatives and its own procurement of 5G services and capabilities around the goal of advancing specialized security capabilities. There are many methods by which the U.S. government can do this, but we recommend focusing on two concrete steps to promote 5G networks with best-in-class security: (1) leveraging the Department of Defense ("DoD") 5G testbeds to advance "Zero Trust Architecture" ("ZTA") in 5G, and (2) eliminating the "lowest price technically acceptable" standard for all federal procurement pertinent to 5G services in all agencies, including DoD, and instead using a balance between lowest price and other critical capabilities such as security to decide on procurement.

Advancing "Zero Trust Architecture" in DoD 5G Testbeds. ZTA avoids blind trust in any internal or external component of the network and instead authenticates everything that connects to or communicates within the network. For specialized and sensitive 5G services, ZTA should become the standard for devices connecting to and applications traversing 5G networks, and it is something 5G networks should seamlessly enable to ensure application layer security.[18] To reach this ambitious goal, Verizon is working through the National Spectrum

[18] In combination with a secure 5G network, Zero Trust Architecture ensures a full stack solution, from fiber to MPLS to MEC to Core to RAN.

Consortium to develop a DoD 5G testbed that will advance both ZTA and domestic software development through MEC. Verizon is creating a secure application platform that rides on top of its secure 5G network, relying on a Software Defined Perimeter ("SDP") to enable this secure 5G overlay that can be managed by partners, including government customers. Verizon's Zero Trust Architecture enables partners to manage access rights, identity, key management, and encryption algorithms within a 5G network slice, which we believe will be valuable in mission-critical 5G use cases in both the private sector and government, ranging from smart cities, to autonomous driving, to smart energy applications. The awards for the first group of DoD 5G testbed facilities will be announced this summer, and Verizon is actively shaping, partnering on, and bidding for these opportunities. We commend DoD and the National Spectrum Consortium for their leadership on these initiatives, and we urge them to leverage the testbeds to advance ZTA.[19]

Eliminating "Lowest Price Technically Acceptable" for 5G Procurement. Section 880 of the John S. McCain National Defense Authorization Act of 2019 requires avoidance of Lowest Price Technically Acceptable ("LPTA") source selection criteria when use would deny the government certain technical and other benefits, particularly in procurements of IT, cybersecurity, telecommunications, and other related services.[20] Verizon supports the ongoing rulemaking to implement this requirement, and as we argued in that proceeding, the government

[19] In addition to its engagement with DoD, Verizon is also teaming with the Department of Energy's Pacific Northwest National Laboratory ("PNNL") to bring 5G Ultra Wideband to its Richland, Washington site. Together, Verizon and PNNL will explore opportunities for 5G to impact some of the world's greatest science and technology challenges in areas like cybersecurity, energy efficiency, and scientific discovery. With Verizon's 5G network onsite, PNNL researchers will test how 5G Ultra Wideband's super-fast speeds and increased bandwidth can enhance emerging tech like machine learning, artificial intelligence ("AI"), and augmented reality and virtual reality ("AR/VR") applications that are used in everything from public safety to computing and analytics. *See* https://www.verizon.com/about/news/verizon-business-national-lab.

[20] Pub. L. 115-232, 41 U.S.C. § 3701.

should issue a final rule that requires avoidance of LPTA in "both DoD and civilian agency procurements."[21] The proposed rule would exclude DoD from this requirement, which risks denying DoD – and its future missions relying on secure 5G services – "the benefits of cost and technical tradeoffs in the source selection process" that Congress plainly intended in Section 880.[22] In short, secure 5G at the DoD and throughout the government should be a cutting-edge service that leverages specialized security capabilities, and should not be subject to the routine procurement standard of "lowest price technically acceptable."

III. U.S. POLICY AT HOME AND ABROAD SHOULD PROMOTE VENDOR DIVERSITY AND ECONOMIC SECURITY

A. A Diverse Bench of Trusted, Global 5G Vendors Is Critical to U.S. Economic Security.

Underlying the development of any secure 5G network is the availability of a diverse, competitive marketplace of trusted vendors of network hardware and software. A wide array of innovation drivers and competitive vendors is an indispensable economic and security imperative for Verizon, for other 5G service providers, and for the United States.[23] In fact, both the Notice and the 5G Strategy underlying it take the fundamental importance of vendor diversity as a

---

[21] Verizon filing to General Services Administration, Letter from Brian R. Kennedy, Sr. Managing Assoc. General Counsel, Public Policy Law & Security (Legal), "Re: Comments on FAR Case 2018-016, Lowest Price Technically Acceptable Source Selection Process" (Dec. 2, 2019).

[22] Pub. L. 115-232, 41 U.S.C. § 3701.

[23] *See, e.g.*, Elsa B. Kania, *Securing Our 5G Future*, Center for a New American Security, Nov. 7, 2019, https://www.cnas.org/publications/reports/securing-our-5g-future ("The U.S. government should explore opportunities to diversify and rebalance its existing dependencies in supply chains and vendors."); Martijn Rasser, *Setting the Stage for U.S. Leadership in 6G*, Lawfare, Aug. 13, 2019, https://www.lawfareblog.com/setting-stage-us-leadership-6g (trusted vendor diversity needed to build secure 5G networks); Lucy Patchett, *UK plans diversification of telecoms supply chain*, CIPS Supply Management, July 23, 2019, https://www.cips.org/supply-management/news/2019/july/uk-plans-diversification-of-the-telecoms-supply-chain/.

given; the Notice does not ask *whether* the U.S. government should "promote 5G vendor diversity and foster market competition" but instead focuses on *how* it should do so.[24]

This challenge must be taken head-on now. To put it bluntly, we risk over the long term lacking the diverse bench of trusted vendors we need to maintain U.S. leadership in the 5G world. It is widely acknowledged that certain foreign companies currently squeeze the global communications network supply chain by undercutting trusted vendors through a mix of aggressive pricing and government supports. This has resulted in dwindling global market share for trusted suppliers of wireless network technologies.

While the Administration is right to acknowledge and confront this economic reality, it must do so via a comprehensive government approach with all agencies and regulators rowing in the same direction. Initiatives could include both bilateral and multilateral efforts to leverage the combined market power of different countries to oppose the non-market supports enjoyed by untrusted vendors. These could include coordinating efforts around international trade and leveraging the combined export financing of like-minded countries to support trusted existing and new entrants in the global marketplace. The U.S. government also should leverage U.S. R&D funding to support funding research into future wireless technologies beyond 5G (*e.g.*, 6G).

---

[24] Notice at 32,017; *see also* National Strategy to Secure 5G of the United States of America at 6-7 (Mar. 2020) ("5G Strategy"), *available at* https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf ("The United States Government will work with the private sector, academia, and international government partners to adopt policies, standards, guidelines, and procurement strategies that reinforce 5G vendor diversity to foster market competition. The United States Government will join private sector and international partners in designing market-base incentives, accountability mechanisms, and evaluation schemas to assess diversity, component transparency, fair financing, and competition across the 5G technology landscape as a means to better secure the global network and protect American values of openness, security, and interoperability.").

The Administration should ensure that federal agencies, and associated private sector initiatives formed in partnership with (or at the request of) government agencies, coordinate and not duplicate efforts. For instance, the ICT SCRM Task Force, organized through the DHS National Risk Management Center, has multiple working groups studying the minimization of risk through vendor selection. Meanwhile, the FCC is exploring means of fulfilling its statutory directive to identifying replacements for vendors and equipment that pose national security risks. The Administration's 5G strategy should be geared toward facilitating coordination between these efforts so that they complement and reinforce each other.

B. Open RAN Holds Promise, But Is Not By Itself Sufficient to Promote Diversity and Competition in the Vendor Market.

As evidenced by Verizon's leadership in the O-RAN Alliance and the Open RAN Policy Coalition, Verizon believes that standards-based open interfaces within Radio Access Networks can help promote a new competitive and diverse market of RAN vendors over the long term. Open RAN is thus a tool to promote vendor diversity and to level the competitive playing field in a RAN market that, as noted above, has become increasingly consolidated in recent years. Carriers need a robust set of competitive options to choose from in the trusted vendor market, and standards-based open and interoperable RAN can help provide those options by making room for smaller players and new combinations of innovative network components from multiple trusted vendors. More broadly, open RAN is fundamentally about innovation, including in software; this is where the future of 5G lies, and where the United States and its allies lead. Verizon therefore encourages the Administration to bear in mind the potential of open RAN as part of the vendor diversity solution.

But we urge policymakers not to rely solely on the promise of open RAN. The strategic imperative of achieving greater supplier diversity will not be solved by open RAN alone in the

face of the strategic government support enjoyed by untrusted suppliers. Policy efforts to advance open RAN must also be accompanied by parallel efforts to enable a more robust and competitive supplier ecosystem both in the United States and globally. We therefore urge the Administration and U.S. allies to continue to coordinate to promote policies that implement the Prague Proposals' call for "open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services."[25] That requires broader policies to ensure a level playing field for all global 5G vendors. The global market represented by the 32 vibrant market democracies promoting these principles constitute a market large enough to sustain a diverse and competitive vendor base; by contrast, U.S. policies that focus narrowly on the domestic U.S. market would fall short. Verizon therefore urges the Administration to take a broad view of policies and private sector and government allies necessary to create and maintain a diverse set of trusted vendors.

[25] The Prague Proposals at 5, https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf; H. Res. 575, § 2 (Jan. 8, 2020) (restating the text of the Prague Proposals).

IV. CONCLUSION

The U.S. strategy for secure 5G must include concrete actions, executable over both the near- and long-term, that will facilitate 5G deployment, leverage private sector advances to promote robust security practices, and develop a diverse and competitive marketplace of trusted, global 5G vendors. The recommendations discussed herein would go far toward achieving these urgent and critical goals.

Respectfully submitted,

/s/ Gregory M. Romano
By: _____

Gregory M. Romano
Christopher D. Oatway
Tamara L. Preiss
VERIZON
1300 I Street, NW
Suite 500 East
Washington, DC 20005
(202) 515-2400

Counsel for Verizon

William H. Johnson
Of Counsel

June 25, 2020