Before the

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

Washington, DC 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G Implementation Plan	)	Docket No. 200521–0144
	)	
	)	

COMMENTS OF
THE OPEN RAN POLICY COALITION

Clete D. Johnson
Wilkinson Barker Knauer, LLP
1800 M Street NW, Suite 800 North
Washington, DC 20036
(202) 383-3405

Counsel to Open RAN Policy Coalition

June 25, 2020

TABLE OF CONTENTS

Before the
NATIONAL TELECOMMUNICATIONS AND
INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
The National Strategy to Secure 5G Implementation Plan	)	Docket No. 200521–0144
	)	
	)	

COMMENTS OF
THE OPEN RAN POLICY COALITION

The Open RAN Policy Coalition[1] submits these comments in response to the Notice and Request for Comments ("Notice")[2] in which the National Telecommunications and Information Administration ("NTIA" or "Administration") seeks recommendations from stakeholders for developing the Administration's Implementation Plan for the National Strategy to Secure 5G, pursuant to the Secure 5G and Beyond Act of 2020.[3] The Coalition and its members believe the Administration has an extraordinary opportunity in this proceeding to inform the forward-looking and game-changing implementation of the National Strategy to Secure 5G.

[1] *See* Open RAN Policy Coalition, https://www.openranpolicy.org. As of this filing, the Coalition includes 45 members, including Airspan, Altiostar, AT&T, AWS, Ciena, Cisco, Cohere Technologies, CommScope, Crown Castle, DeepSig, Dell Technologies, DISH Network, Facebook, Fujitsu, Google, Hewlett Packard Enterprise, IBM, Intel, JMA Wireless, Juniper Networks, Marvell Technology Group, Mavenir, Microsoft, NEC Corporation, NewEdge Signal Solutions, Nokia, NTT, Oracle, Parallel Wireless, Pivotal Commware, Qualcomm, Quanta Cloud Technology, Radisys, Rakuten, Reliance Jio, Robin.io, Samsung Electronics America, Telefónica, U.S. Cellular, US Ignite, Verizon, VMWare, Vodafone, World Wide Technology, and XCOM-Labs.

[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).

[3] Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129, 134 Stat. 223 (2020), https://www.congress.gov/116/plaws/publ129/PLAW-116publ129.pdf.

Introduction

The Coalition represents a diverse group of companies formed to promote initiatives and policies that will advance the adoption of open and interoperable solutions in the wireless Radio Access Network (RAN) as a means to promote innovation, spur competition, and expand the supply chain for advanced wireless communications technologies, including 5G. Coalition members represent a cross-section of the wireless communications industry, ranging from network operators to network solutions providers, systems integrators, cloud providers, edge device manufacturers, and others.

Coalition members believe that by standardizing or "opening" the protocols and interfaces between the various subcomponents (*e.g.*, radios, hardware and software) in the RAN, networks can be deployed with a more modular design without being dependent on a single supplier. Developing, standardizing, and validating open interfaces will allow secure and reliable interoperability across different market players, lower the barrier to entry for new innovators, and lower the cost of adoption by service providers. We believe that there are a variety of steps that policymakers can take to facilitate a vibrant marketplace of suppliers and increased adoption of new innovation based upon open interfaces. In order to nurture this technological approach and accelerate stable, sustainable, and successful advances, the Coalition promotes initiatives and policy priorities that (1) support new and existing innovative technology suppliers that are implementing these open interfaces, as well as small and large network operators, (2) help create a competitive global ecosystem of diverse trusted suppliers and service providers, and (3) build and maintain U.S. and allies' technological leadership both in 5G and future wireless network development.

In these comments, the Coalition addresses the central aim of this proceeding in general and the Secure 5G and Beyond Act's requirements in particular – namely, that it is a national security imperative that U.S. and allied communications networks provide secure and reliable connectivity. The open and interoperable RAN solutions that are being deployed today in major markets in other parts of the world are poised for deployment in the United States; additionally, these solutions provide the secure and reliable networks that are the goal of the National Strategy to Secure 5G and related proceedings. Moreover, their openness and interoperability provide a platform that facilitates future upgrades in security and reliability with greater efficiency and reduced maintenance demands as innovation continues in this field.

The Coalition urges the Administration to (1) encourage open and interoperable RAN in implementing all Lines of Effort of its National Strategy to Secure 5G, and (2) take urgent policy actions to advance open and interoperable RAN in a manner that promotes flexibility in the near-term, and innovation and market diversity over the long-term. We outline these recommendations below.

I. The Open RAN Policy Coalition Recommends that the Administration Leverage Open and Interoperable RAN as a Driver of Innovation and Market Diversity in Implementing the National Strategy to Secure 5G.

The United States and its allies have an opportunity to leverage this moment in technological development to make an enormous leap toward the future of secure and reliable networks. It is imperative – both in the immediate near future and over the longer term – that network operators in the United States and worldwide which are investing in new infrastructure and network upgrades through the transition to 5G have a competitive and diverse set of choices among innovative and trusted suppliers providing secure 5G. Open and interoperable RAN provides operators this set of choices.

A. *Open and Interoperable RAN Provides a Secure Network.*

Open and interoperable interfaces, defined in technical specifications, provide a foundation and architecture for improving security. First, on a basic level, the ability to have a more modular design, with different suppliers providing different components of the network, can enhance security by allowing operators to more quickly replace or address network problems, including suspect equipment. Further, a more intelligent RAN will enable operators to deploy security capabilities closer to the network edge, allowing operators to more quickly respond to threats and shift network capacity on demand. Open architecture also allows operators to choose and apply up-to-date security patches available for Commercial Off the Shelf (COTS) components deployed in their networks (e.g., operating systems, Network Function Virtualization infrastructure, Basic Input/Output System firmware, etc.) and to address security vulnerabilities proactively. These developments, while different from traditional deployments, will improve network security. Although operators procure and integrate open RAN network functions in new ways, operators bring the same expertise, diligence, and requirements for security and resilience to these environments. In short, open RAN provides the framework for these communications network stakeholders to align on shared understanding of security requirements and to tailor security requirements at a more granular level than has been possible before.

Additionally, 5G and an open RAN also enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers, and network operators to assess and to manage security risks. Because an open RAN is a fundamentally open architecture, it opens the ecosystem to new suppliers, increasing the diversity of virtualized RAN solutions. Network enhancements inherent to 5G architectures, such as Multi-Access Edge Computing

(MEC), provide the opportunity for improved security by enabling capabilities presently deployed in core networks, such as network monitoring for security threats, to be pushed closer to the edge. Network slicing can also enable isolated network capacity for highly critical use cases separate from general Internet traffic. Open interfaces also support more virtualized network functions, enabling additional security controls through micro-segmentation and containerization. While 5G delivers many breakthrough benefits, security is the first priority, not an afterthought. 5G networks introduce advanced security features, which include enhanced subscriber privacy, secure communications, and secure intra-operator and inter-operator communications. 5G networks also bring significant security enhancements in multiple areas outlined below that also pertain to open RAN.

i. Standards Drive Transparent and Vetted Security, Interoperability and Trust.

Standards play an important role in 5G security and an open RAN. As discussed in greater depth below in Section I.B, the opportunity to build open, interoperable and standards-based 5G networks has already begun to spur innovation and competition among diverse companies worldwide, enabling greater security for 5G. Standards development organizations, including but not limited to 3GPP, GSMA, ETSI, the O-RAN Alliance, and the Telecom Infrastructure Project (TIP), help grow the ecosystem by enabling new and existing technology providers and wireless carriers to rapidly align on security requirements.

Open standards help users and network operators better understand, align on, and demonstrate successful implementation of security requirements. This effectively grows the market for 5G solution suppliers as network operators have the option to choose from a variety of suppliers, increasing the opportunity for solutions providers to offer standardized solutions to many operators, instead of developing unique, one-off solutions for individual operators. Most importantly, operators and suppliers can coordinate new information about threats, vulnerabilities, and exploits, allowing greatly accelerated development and deployment of mitigations.

ii. Cloud Architecture Ensures Resilience, Scalability and Segmentation and Allows the Introduction of Multi-Access Edge Computing (MEC).

5G is built on cloud architecture – the same cloud architecture that is the bedrock of today's internet and the public cloud. Cloud architecture allows for rapid, standards-based deployment of infrastructure as needed. It is a far more scalable and dynamic approach than the long cycles needed to develop, test, deploy, and configure for fixed function network appliances. For example, in response to live traffic on the 5G network, with a cloud architecture, the 5G core can immediately detect the need, and automatically provision and deploy capabilities as needed. Network operators have seen this dynamic play out as they provision their networks in response to the unprecedented demands placed on networks during COVID-19. These developments will increase network resiliency.

5G cloud architecture also facilitates improved network segmentation, allowing grouping and separation of security sensitive network functions. The same architecture allows the deployment and lifecycle management of entire use cases using "network slicing." Because a network slice is effectively a complete end-to-end network, each slice will include security appropriate to its own requirements and can be developed and deployed as a slice. Different network slices can also run side by side for different purposes and have their own security requirements applied to meet their respective needs.

The 5G architecture also introduces new security capabilities including: (1) leveraging MEC to collate and process sensor traffic at a factory, or to shift Distributed Denial of Service (DDoS) detection and mitigation to the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact; (2) strengthening encryption to 256-bit end-to-end encryption for the over-the-air interface and encryption of each device's International Mobile Subscriber Identity (IMSI) to further secure consumer device-specific information; and (3) establishing a security edge protection proxy that will mitigate vulnerabilities in prior technology (e.g., SS7 and Diameter) and attacks when subscribers are roaming between different carriers' networks.

iii. Segmentation, Containerization and Virtualization Provide Enhanced Security and Isolation from the Hardware Up.

An open RAN takes advantage of the migration towards software-based networks and virtualization. These are concepts that have been deployed in networks for several years in the core and backbone networks and are now being increasingly introduced in the RAN. A software-based network moves the network functions to software as opposed to the past, where network operators would deploy purpose-built physical appliances for network functions. Software-based functions and virtualization enable the replacement of costly, purpose-built hardware devices with general purpose servers found in every cloud data center. From a security perspective, software-based networking and virtualization enables additional security techniques such as sandboxing, micro-segmentation, containerization, and network slicing. There are also important trust and security capabilities of virtualization enabled by modern hardware and processors. The end result is that through advancements in hardware and virtualization, operators have more tools to ensure the security and resilience of the network.

B. Open and Interoperable RAN Solutions are Presently Ready to Deploy.

Open RAN specifications allow innovative companies to develop products, software solutions, and reference designs in a diverse and competitive global market. Large and small network operators are conducting trials, and interoperability testing has begun. Several operators are starting to trial and deploy open interfaces based on O-RAN Alliance specifications.[4] Open RAN systems built to shared and open specifications are already deployed; as described below, the NTT Docomo and Rakuten deployments in Japan are prominent examples, as are deployments by major European operators, Telefonica and Vodafone. While global standards are important to create opportunities for interoperability of scalable solutions, open interface specifications further maximize the potential to innovate and compete in virtualized infrastructure.

i. Standards and Specifications for 5G and Open RAN are Developing in Parallel.

Global 5G specifications are being developed within the 3rd Generation Partnership Project (3GPP). 3GPP specifications are structured as "Releases" on a 15-to-18-month cadence. 3GPP Release 15, providing the first 5G enhanced mobile broadband capabilities, was approved in June 2019. Release 16, which adds functionality for mission critical applications and massive IoT, is nearing finalization. Release 16 completes 3GPP's submission into the ITU-R for consideration as a candidate radio interface technology for IMT-2020. 3GPP specifications include interfaces between specific elements within the RAN, within the core network, and between the RAN and the core network. The existence of open and interoperable interfaces is key to disaggregating the network and to promoting a diverse ecosystem of vendors in the cellular infrastructure market.

While the 3GPP process focuses on the global specifications, the openness of the interfaces between specific elements within the RAN or core network is key to disaggregating the network and facilitating additional suppliers in entering the wireless infrastructure market.

[4] The O-RAN Alliance and its members, many of whom are also members of the Open RAN Policy Coalition, are developing the technical specifications that enable open and interoperable RAN. *See* O-RAN Alliance, https://www.o-ran.org.

The O-RAN Alliance and other consortia such as TIP are developing specifications for these open interfaces, complementary to standards promoted by 3GPP. The O-RAN Alliance has developed specifications for certain RAN interfaces that had not been addressed by 3GPP.

Key specifications, such as the fronthaul specification that defines the interface between the radio and the baseband unit of the RAN, have been completed by the O-RAN Alliance. Additional O-RAN Alliance specifications such as software testing and machine learning applications, will be available in the 2nd quarter of 2020. Similar to 3GPP, ongoing evolutions of O-RAN Alliance specifications will continue. For example, the end-to-end system test specification is expected to be released in August. TIP also has several project groups developing technologies for open RAN and has recently formed a partnership with the O-RAN Alliance.

The goal of open interfaces is to avoid a “lock-in” effect where proprietary or semi-proprietary implementations inhibit competition among suppliers. The end result is that operators have greater options to mix equipment from different suppliers in the same RAN, and other layers of the network, providing greater flexibility and lower costs and which enables a vibrant ecosystem of suppliers driving innovation.

ii. Open RAN Networks are Currently Deployed.

There are multiple different real-world implementations of Open RAN underway today, ranging from deployments to trials, demos, and standards development activity. Examples of network and software deployments include the following:

- Rakuten has deployed a commercial fully cloud-native mobile network with open virtualized RAN (vRAN) in Japan, with radios and other equipment, software, and services from multiple vendors both in 4G and 5G.

- Altiostar has deployed its software with 4G/5G radios from Airspan, MTI, Nokia and Sercomm and is working with radios and related equipment and materials from Flex, Fujitsu, KMW, NEC and Xilinx to deploy by mid-year.

- On April 29, 2020, Indian integrated telecommunications services provider, Bharti Airtel, announced that it had deployed Altiostar's open vRAN solution across multiple major cities in India.

- DISH Network is building the United States' first software-defined 5G wireless broadband network utilizing an open, intelligent RAN architecture. DISH has entered into a multi-year agreement with Mavenir to deliver cloud-native open RAN software.

- Mavenir has deployed with Vodafone Idea.

- NTT DOCOMO has already realized interoperability between base station equipment of Fujitsu, NEC, and Nokia with O-RAN Alliance-compliant fronthaul and X2 interfaces in their 5G commercial service.

- Telefónica has established an Open RAN consortium of hardware and software companies aimed for the development and deployment of open RAN in 4G and 5G, comprising the necessary design, development, integration, operation, and testing activities required to materialize Open RAN.

- Since February 26, 2018, when JMA Wireless announced its open vRAN and work with Telecom Italia, it has since has deployed multi-operator, open, virtualized RAN in multiple locations across multiple operators, in both outdoor dense city networks and large-scale venues such as stadiums, and within buildings for private wireless use, providing validation of implementation and scale of vRAN software in real-world use.

- Parallel Wireless, Mavenir, and Altiostar have been deploying Open RAN for years with operators such as Vodafone, Telefonica, MTN, Optus, and they are strategic partners for rural U.S. operators and members of the Competitive Carriers Association (CCA).

In addition to these real-world deployments, the following trials, demonstration projects, and standards development activities are presently underway:

- AT&T is one of the founding members and currently chairs the O-RAN Alliance. AT&T has also conducted several demos and trials including working with CommScope and Intel to demonstrate a mmWave 5G gNB and open fronthaul leveraging developments at O-RAN.

- Verizon contributes as an active O-RAN Alliance Board member and Working Group co-chair to advance the open interface model with a wide range of ecosystem stakeholders, while, in parallel, partnering with key suppliers to successfully conduct vRAN trials as a move to hardware-agnostic solutions.

- Vodafone is currently chair of TIP and has active trials of Open RAN ongoing in Turkey, Mozambique, DRC, Ireland, and UK with Parallel Wireless and Mavenir.

- AT&T recently hosted the O-RAN Alliance Plugfest in New York City, where Samsung demonstrated the multi-vendor compatible Configuration, Performance, and Fault Management capabilities of the O1 interface.

- Telefónica conducted in 2019 successful open RAN trials in Brazil based on 4G, which are being evolved in 2020 to more ambitious 4G/5G trials towards 4G/5G commercial deployments.

- VMware, Inc. and Deutsche Telekom recently announced the companies are collaborating on an open and intelligent vRAN platform running on Intel servers, based on O-RAN Alliance specifications, to bring agility to RANs for both existing LTE and future 5G networks.

- Jio is working with a group of operators and vendors to develop an Open Test and Integration Centre (OTIC) for commercializing O-RAN compliant disaggregated 5G access infrastructure and defining an end-to-end test framework specification that will be released in August 2020. Jio is currently testing multiple O-RAN compliant, disaggregated and virtualized RAN solutions in its labs.

- Radisys is helping accelerate the open RAN ecosystem by working closely with various ecosystem partners for both mmWave and sub-6 GHZ solutions. Radisys RAN software is powering numerous NEPs trials/deployments with open RAN architecture across the globe.

Through the implementation of the National Strategy to Secure 5G, the Administration has the opportunity to advance the deployment of open and interoperable RAN solutions in a wide variety of network environments throughout the United States, facilitating economies of scale. The Coalition urges the Administration to leverage these possibilities in implementing all four Lines of Effort of the National Strategy to Secure 5G, including through the policy actions we recommend below.

II. Implementation of the National Strategy to Secure 5G Should Include Urgent Actions to Advance Open and Interoperable RAN in a Manner that Promotes Flexibility in the Near-Term and Innovation Over the Long-Term.

With the above background in mind, the Coalition provides below its thoughts on the key opportunities to leverage open and interoperable RAN in its implementation of the National Strategy to Secure 5G. As we recommended to the Federal Communications Commission (FCC) in its ongoing proceeding to identify and replace "covered communications equipment and services," we believe the Administration should "further[] the flexibility and innovation that has yielded a diverse array of suppliers, a wide range of vibrant services, and enormous technological strides."[5] The Administration should broadly promote these innovations and possibilities with a general support for the open and interoperable standards based on rigorous technical research and testing that the United States and its allies have long spearheaded, but it should not specify or seek to prescribe the future development of the 5G ecosystem.[6]

Immediate Actions. The Coalition urges the Administration – and, where necessary, Congress – to undertake the following actions as soon as possible to implement the National Strategy to Secure 5G.

[5] Comments of The Open RAN Policy Coalition, WC Docket No. 18-89 at 7-8 (filed May 20, 2020) (stating "First, the Commission should develop a list of categories of suitable replacement equipment and services, rather than a list of specific named suppliers or particular equipment and services… Second, the list should include all pertinent categories of equipment and services from lawfully eligible suppliers, and the list should not include the precise names of any equipment and services… Third, the list should include suppliers of Open RAN solutions and virtual network equipment and services.").

[6] As we noted in our comments in that proceeding, the FCC opposes such prescriptive technology choices by the government. *See, e.g.*, Remarks of FCC Chairman Ajit Pai at the 7th Congreso Latinoamericano De Telecomunicaciones, Caroba, Argentina (July 3, 2019) ("The FCC does not pick winners and losers in our domestic marketplace, and we carry that same philosophy forward internationally."); *Deployment of Wireline Services Offering Advanced Telecommunications Capability*, Memorandum Opinion and Order and Notice of Proposed Rulemaking, 13 FCC Rcd 24012 ¶ 2 (1998) ("The role of the Commission is not to pick winners or losers, or select the 'best' technology to meet consumer demand, but rather to ensure that the marketplace is conducive to investment, innovation, and meeting the needs of consumers.").

First, provide at least $1 billion and up to $2 billion in new funding to effectuate the FCC's implementation of the replacement of "covered communications equipment and services" under Section 4 of the Secure and Trusted Communications Networks Act. The Coalition recommends that Congress specify that a portion of this funding should be reserved for recipients who elect to use the funding to deploy open RAN network equipment that supports open and interoperable standards in the RAN consistent with specifications defined in the O-RAN Alliance and TIP, starting the migration to open standards-based compatible equipment within two years. This funding should also recognize that operators applying for this funding will need flexibility to enable interoperability with legacy systems.

Second, Congress should immediately enact legislation to support and fund open and interoperable RAN solutions by authorizing and appropriating two robust new funds: (1) An innovation fund of at least $1 billion to spur research and development and deployment towards open-architecture, software-based wireless technologies, funding innovative, "leap-ahead" technologies in the U.S. mobile broadband market; and (2) a multilateral global fund of at least $750 million to work with U.S. foreign partners to accelerate the adoption of trusted and secure equipment globally and encourage multilateral participation.

Third, the Department of Defense (DoD) should use its own 5G enhancements and the National Spectrum Consortium 5G testbeds to promote open and interoperable RAN. In particular, the Secretary of Defense should direct pertinent DoD personnel to (1) incorporate open and interoperable RAN in some portions of its future 5G programs both stateside and abroad *(e.g.,* use a portion of its authorization to spend up to $275 million on Next Generation Information Communications Technology such as 5G to deploy interoperable network technology in connection with implementation of Section 226 of the FY2020 National Defense

Authorization Act); (2) accelerate DoD programs, such as future National Spectrum Consortium 5G testbeds, to ensure open RAN solutions are incorporated in the FY2020 and FY2021 time periods; and (3) use DoD procurement authority to test and/or deploy 5G open and interoperable interface-based networks through the 5G to NextG solicitation (6-12 months out).

Fourth, the U.S. government should undertake a multipronged effort to facilitate and accelerate deployment of 5G. In order to maintain a deployment edge, the spectrum pipeline for 5G is essential to advancing U.S. networks and driving deployment of new technological solutions, including those that utilize open and interoperable RAN solutions. In particular, we must ensure there is no delay in the planned December 8, 2020 launch of the FCC spectrum auction for the mid-band frequencies in 3.7-3.98 GHz band and encourage the U.S. to quickly identify and bring to market additional mid-band spectrum for 5G deployment.

Fifth, accelerate growth of open and interoperable RAN internationally. To effectively promote a diverse, competitive supply chain of trusted, secure, open and interoperable technologies, the National Strategy to Secure 5G should: (1) leverage U.S. international funding agencies (e.g., EXIM Bank, U.S. International Development Finance Corporation, USAID), and the State Department, to develop incentives or include preferences for open and interoperable equipment in wireless projects that will result in the deployment of such network equipment from trusted vendors and service providers; (2) prioritize open and interoperable RAN advancement in the Indo-Pacific Strategy with enhanced funding; (3) encourage deployments in other markets, including India and Brazil; (4) fund international collaboration such as joint research and development programs; (5) coordinate with like-minded countries to adopt similar policies such as supporting open and interoperable RAN solutions from trusted vendors and service providers with their government funding sources; and implementing the widely accepted Prague Proposals calling for "open, interoperable, secure standards, and industry best practices to promote a vibrant and robust cyber security supply of products and services."

Additional Actions. More broadly, the Coalition urges the Administration – and, where necessary, Congress – to undertake the following actions as well to implement the National Strategy to Secure 5G over the long term.

First, in federal procurement, agencies should establish procurement preferences for open, interoperable and standards-based equipment. Examples include: (1) as recommended above, DoD should use its procurement authority to test and/or deploy open and interoperable networks; (2) successful programs from FY2020 and FY2021 should be expanded in both scope and scale as quickly as possible and transitioned into programs of record. Potential partners to expand open RAN include: DARPA, Spectrum Forward Consortium, AFWERX, NavalX, and Army Futures Command; and (3) the Department of Energy should promote open and interoperable interface-based networks using its procurement authority for spectrum development projects through the Idaho National Laboratory, the Pacific Northwest Laboratory, and others.

Second, regarding research and development, the Administration should incentivize establishment of a trusted U.S. and allied supply chain and technology innovation through research and development. Examples include: (1) fund 5G innovation based on open, interoperable standards, including open and interoperable RAN (*e.g.*, as recommended above, through DARPA); (2) incentivize expansion of a trusted vendor radio equipment supply chain (including manufacturing) through research and development tax credits and other investment incentives; (3) incentivize expansion of trusted vendors developing open and interoperable RAN technology by utilizing public/private partnerships such as In-Q-Tel; (4) create a long term pipeline of funding for continued development of open and interoperable RAN (beyond presently pending bills); and (5) design a program to incentivize investment and job creation in the United States by offering research and development credits and other incentives for network technology suppliers.

Conclusion

Open and interoperable RAN solutions are real and available today for deployment via suppliers and their systems integration partners, and as such they are part of the diverse supplier market that can advance the security and reliability of U.S. and global communications networks through the National Strategy to Secure 5G. Operators and policymakers who may not yet be fully aware of the viability of these solutions should be advised that these options are among the technology choices that are available to them. The National Strategy to Secure 5G should leverage all its Lines of Efforts to amplify the diversity of technological options that is emerging today. The Coalition and its members look forward to working with the Administration on this important and promising proceeding.

Respectfully submitted,

OPEN RAN POLICY COALITION

By: /s/ Clete D. Johnson

Clete D. Johnson
Wilkinson Barker Knauer, LLP
1800 M Street NW, Suite 800 North
Washington, DC 20036
(202) 383-3405

Counsel to Open RAN Policy Coalition

June 25, 2020