Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Applicability of Section 4 of the Secure Networks	)	WC Docket No. 18-89
Act to the Rulemaking on Protecting Against	)	DA 20-406
National Security Threats to the	)	
Communications Supply Chain	)	

COMMENTS OF THE OPEN RAN POLICY COALITION

Diane Rinaldo
Executive Director

OPEN RAN POLICY COALITION
P.O. Box 63344
Farragut Post Office
1800 M Street NW FRNT 1
Washington, DC 20033
(202) 747-4041

May 20, 2020

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Applicability of Section 4 of the Secure Networks	)	WC Docket No. 18-89
Act to the Rulemaking on Protecting Against	)	DA 20-406
National Security Threats to the	)	
Communications Supply Chain	)	

COMMENTS OF THE OPEN RAN POLICY COALITION

The Open RAN Policy Coalition ("Coalition")[1] is pleased to submit these comments in the above-captioned proceeding – its first public filing since its establishment on May 4, 2020 – in order to aid the Federal Communications Commission ("Commission") as it develops a framework to replace equipment and services in eligible operators' networks.[2] The Coalition and its members believe the Commission has an extraordinary opportunity in implementing the Secure and Trusted Communications Networks Act ("Secure Networks Act") to promote innovation in secure and reliable networks.

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

[1] *See* https://www.openranpolicy.org/. As of this filing, the Coalition includes 31 members, including Airspan, Altiostar, AT&T, AWS, Cisco, CommScope, Dell, DISH Network, Facebook, Fujitsu, Google, IBM, Intel, Juniper Networks, Mavenir, Microsoft, NEC Corporation, NewEdge Signal Solutions, NTT, Oracle, Parallel Wireless, Qualcomm, Rakuten Mobile, Samsung Electronics America, Telefónica, US Ignite, Verizon, VMWare, Vodafone, World Wide Technology, and XCOM-Labs.

[2] Public Notice, *Applicability of Section 4 of the Secure Networks Act to the Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, DA 20-406, WC Docket No. 18-89 (rel. Apr. 13, 2020) ("Public Notice").

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 (radios, hardware and software) in the RAN, networks can be deployed with a more modular design without being dependent on a single supplier.

Developing and standardizing open interfaces will allow secure and reliable interoperability across different market players and lower the barrier to entry for new innovators. We believe that there are a variety of steps that policymakers can take to facilitate a vibrant marketplace of suppliers 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 technology suppliers, 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 Commission proceeding in general and the Secure Networks Act's requirements in particular – namely, that it is a national security imperative that U.S. communications networks provide secure and reliable connectivity. The open and interoperable RAN solutions that are being deployed today in major markets all over the world are poised for deployment in the United States, including through the replacement program proposed in this proceeding; additionally, these solutions provide the secure and reliable networks that are the goal of the overall proceeding. 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. To that end, the Coalition believes that the Commission should implement its responsibilities under the Secure Networks Act by developing a reference list of categories of replacement equipment and services to aid carriers in their replacement decisions; that this list should broadly include all relevant categories of equipment and services, including open RAN and virtual solutions; and that while the Commission should indeed leverage this proceeding to give new solutions an opportunity for deployment, the Commission should not pick winners nor mandate replacement decisions.

I. The Open RAN Policy Coalition Recommends that the Commission Use This Proceeding to Advance Network Security by Promoting Innovation and Market Diversity.

The Commission has an opportunity to use this one-time replacement program for regional carriers to make an enormous technological leap toward the future of secure and reliable networks. Network operators eligible for replacement under the Secure Networks Act often operate in challenging geographical environments with low margins, where the need for a competitive and diverse set of choices among innovative and trusted suppliers is most important. 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 security. Although operators procure and integrate Open RAN network elements in new ways, operators bring the same expertise, diligence and requirements for security and resilience to these environments. Open RAN also enables new capabilities and control points that enable suppliers, test equipment manufacturers, systems integrators, and wireless network operators to assess and to manage security risks. 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.

These developments, combined with Mobile Edge Computing (MEC), can help facilitate capabilities such as "network slicing" that enable specific network capacity, distinct from general Internet traffic, for particular categories of use. For example, for Internet of Things devices, open interfaces and MEC can enable detection and mitigation of Distributed Denial of Service (DDoS) attacks closer to the edge of the network. Open interfaces will support more virtualized network functions, enabling additional security controls through micro-segmentation and containerization. The combination of micro-segmentation and strong authentication are common practices today in enterprise security management.

Open RAN's open interfaces are defined transparently in technical standards bodies, built on battle-hardened methods for protecting the cloud, and rooted in proven hardware virtualization technology. 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.

b. ***Open 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, and several carriers are starting to trial and deploy open interfaces based on O-RAN Alliance specifications.[3] 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. Global 5G specifications are being developed within the 3rd Generation Partnership Project (3GPP). 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 creating additional suppliers in the cellular infrastructure market. The O-RAN Alliance and other consortia such as the Telecom Infra Project (TIP) are developing specifications for these open interfaces, complementary to standards promoted by 3GPP, to enable such next generation open RAN infrastructures but many interfaces remain closed or proprietary. Openness seeks to avoid defining key interfaces in proprietary or semi-proprietary ways that may inhibit competition among suppliers. The result of specifications with open interfaces is operators have greater options to mix equipment from

[3] 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* https://www.o-ran.org/.

different suppliers in the same RAN, and other layers of the network, providing greater flexibility and lower costs.

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. Additional specifications will be completed in 2020; the end-to-end system test specification is expected to be released in August.

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 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 from Flex, Fujitsu, KMW, NEC and Xilinx to deploy by mid-year.

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

- Mavenir has deployed with Vodafone Idea and is partnering with DISH Network to deploy a fully virtualized nationwide network with Open RAN in the United States.

- 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.

- 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 virtualized RAN 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 virtual RAN (vRAN) platform running on Intel servers, based on O-RAN Alliance specifications, to bring agility to radio access networks (RANs) for both existing LTE and future 5G networks.

Through this proceeding and replacement program, the FCC has the opportunity to enable the deployment of open and interoperable RAN solutions in a wide variety of network environments throughout the United States, facilitating economies of scale.

II. The FCC Should Develop a List of Replacement Categories in a Manner that Promotes Flexibility in the Near-Term and Innovation Over the Long-Term.

With this background in mind, the Coalition provides below its responses to what we perceive to be the central questions identified in the Public Notice. These responses are uniformly premised on our belief that the Commission should approach its statutory mission with an eye toward furthering the flexibility and innovation that has yielded a diverse array of suppliers, a wide range of vibrant services, and enormous technological strides. The Commission should eschew any invitation or temptation to use this moment as an opportunity to specify or prescribe the future development of the 5G ecosystem.

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. Importantly, the statute does not prescribe a specific path or format for the Commission to follow in compiling a "list" to guide the replacement process. On the contrary, Section 4(d)(1) empowers the Commission to develop a list of either "suggested replacements" or "categories of replacements."[4] The Commission should embrace the latitude given to it by Congress and focus its efforts on the latter option. By describing categories of replacement services and equipment rather than specifying individual pieces of equipment or select services, the Commission will facilitate operators' navigation of the wide variety of choices they have available to them through this replacement program, while also empowering them to make their own discerning choices about what solutions are best for their particular needs – rather than inserting the Commission into that decision-making process.

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. Although existing narrow prohibitions on the use of equipment and services have involved naming specific companies (including the ban on suppliers that the Commission is now implementing in this proceeding), the Commission should reject that

[4] Pub. L. 116-124, 133 Stat. 158, § 4(d)(1) (2020).

methodology for identifying the far broader array of suitable replacements. Such an approach would effectively constitute a mandate to use certain suppliers or types of equipment, putting the Commission in a position it has repeatedly (and properly) disavowed: that of picking winners and losers in the marketplace.[5] Doing so would also limit choice and innovation over time. Moreover, an approach premised on identifying specific suppliers or equipment would reflect little more than a snapshot of the marketplace as it exists at the time, and would quickly become outdated as this dynamic market creates new innovations.

Instead, the Commission should issue a general guide to the categories of choices available in the market for replacement purposes. This guide should broadly include all categories of offerings available on the market today – including open RAN solutions.

Third, the list should include suppliers of Open RAN solutions and virtual network equipment and services. In addition to the Open RAN solutions described in these comments – and often as complementary elements of those Open RAN solutions – there are numerous secure and cost-efficient virtual network solutions available on the market now. Open RAN refers to open and interoperable interfaces within and between the various subcomponents of the RAN, namely the radio, hardware or baseband unit and software. In Virtualized RAN, much of the RAN or network function is virtualized in software. There is an ongoing move towards Software Defined Networking (SDN) and Network Function Virtualization (NFV) which take advantage

[5] *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.").

of open and standardized interfaces. However, the Coalition notes that Open RAN and interoperable RAN interfaces and protocols do not require that all elements in the RAN be software-based. In order to scale Open RAN and attract new entrants, protocols and interfaces need to be open, interoperable and standardized. Which elements become software or "virtual" is an implementation issue that will be addressed by individual operators and their supplier partners.

In any case, both open and virtualized 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. communications networks through this proceeding. Operators that may not yet be fully aware of the viability of these solutions should be advised that these options are among the choices that are lawfully available to them. In this respect, the Commission can advance 5G by ensuring that the "category of replacements" is comprehensive, thereby serving as a reference information resource and amplifying the diversity of technological options that is emerging today.

Conclusion

The Coalition and its members look forward to working with the Commission on this important and promising proceeding.

/signed/ Diane Rinaldo

Diane Rinaldo
Executive Director

OPEN RAN POLICY COALITION
P.O. Box 63344
Farragut Post Office
1800 M Street NW FRNT 1
Washington, DC 20033
(202) 747-4041

May 20, 2020