

FCC FACT SHEET^{*}
Promoting the Deployment of 5G Open Radio Access Networks
GN Docket No. 21-63

Background: The Commission has a duty to protect the safety of life and property and promote the national defense through wire and radio communication, as well as to encourage new technologies and services. Some parties assert that open radio access networks (Open RAN) are a potential path to drive 5G innovation, with industry proponents arguing that it could provide opportunities for more secure networks, foster greater vendor diversity, allow for more flexible network architectures, lower capital and operating expenses, and lead to new services tailored to unique use cases and consumer needs; others contend that Open RAN is still in its most formative stages, and that while promising, significant work remains before the benefits of the concept can fully be realized.

This Notice of Inquiry seeks input on the status of Open RAN and virtualized network environments: where the technology is today and what steps are required to deploy Open RAN networks broadly and at scale. It also seeks comment on whether and, if so, how deployment of Open RAN-compliant networks could further the Commission's policy goals and statutory obligations, advance legislative priorities, and benefit American consumers by making state-of-the-art wireless broadband available more quickly and to more people in more parts of the country.

What the Notice of Inquiry Would Do:

- Describe the relationship of recent government action to Open RAN development, including through Commission and other U.S. government action, legislative developments, and international activity.
- Seek comment on the current status of Open RAN development and deployment domestically and internationally.
- Seek comment on potential public interest benefits in promoting Open RAN development and deployment, including increased competition, network vendor diversity, affordability for consumers, network security and public safety, and other potential benefits.
- Seek comment on additional considerations regarding Open RAN development and deployment, including potential software vulnerabilities or risks posed by a virtualized operating environment.
- Seek comment on barriers to Open RAN development and deployment and whether and what Commission efforts could be undertaken to promote Open RAN development and deployment.
- Seek comment on how the Commission can collaborate with and/or leverage ongoing Open RAN research and development activities in academia and other federal agencies.
- Discuss and seek comment on the costs and benefits of Open RAN deployment.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in GN Docket No. 21-63, which may be accessed via the Electronic Comment Filing System (<https://www.fcc.gov/ecfs>). Before filing, participants should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR § 1.1200 *et seq.*

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
Promoting the Deployment of 5G Open Radio) GN Docket No. 21-63
Access Networks)

NOTICE OF INQUIRY*

Adopted: []

Released: []

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #
I. INTRODUCTION..... 1
II. BACKGROUND..... 4
A. Open RAN Development and Future Use..... 5
B. Recent U.S. Government Actions Related to Supply Chain and Network Security..... 11
1. Commission Orders and Actions..... 11
2. Recent Legislation..... 18
3. Other Government Actions 22
III. DISCUSSION 23
A. State of Development and Deployment of Open RAN Solutions..... 23
B. Potential Public Interest Benefits in Promoting Development and Deployment of Open RAN..... 30
1. Increased Competition and Network Vendor Diversity 30
2. Affordability of Services and Products for Consumers..... 36
3. Network Security and Public Safety..... 37
4. Potential Technological Benefits of Open RAN Deployment..... 41
C. Additional Considerations Regarding Open RAN Development and Deployment..... 47
1. Disaggregation/Need for a System Integrator 47
2. Network Security and Public Safety..... 49
3. Open-Source Software Vulnerabilities..... 53
4. Risks of a Virtualized Operating Environment 54
5. Barriers to Adoption by Established Operators..... 56

* This document has been circulated for tentative consideration by the Commission at its March, 2021 open meeting. The issues referenced in this document and the Commission’s ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Acting Chairwoman has determined that, in the interest of promoting the public’s ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC’s ex parte rules apply and presentations are subject to “permit-but-disclose” ex parte rules. See, e.g., 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission’s ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission’s meeting. See 47 CFR §§ 1.1200(a), 1.1203.

6. Other Considerations..... 57

D. Potential Commission Efforts to Promote Development and Deployment 58

1. Identify Potential Barriers 58

2. Testbeds and Demonstration Projects 60

3. USF/Rip and Replace 63

4. Operational/Service Rules..... 69

5. Commission Outreach and Information Gathering 71

6. Legal Issues 80

E. Costs and Benefits of Open RAN Deployment 83

IV. PROCEDURAL MATTERS..... 86

V. ORDERING CLAUSES..... 91

I. INTRODUCTION

1. In creating the Federal Communications Commission (FCC or Commission), Congress charged the agency with protecting the safety of life and property and promoting the national defense through wire and radio communication.¹ Over the last decade, actions by Congress, the Executive Branch, and the Commission have repeatedly stressed and prioritized supply chain risk management and the deployment of secure and reliable networks in the United States. The Commission has worked closely with its federal partners on this critical issue and has acted decisively to secure our communications networks and the communications supply chain. Congress has also established that it is “the policy of the United States to encourage the provision of new technologies and services to the public.”²

2. Some parties assert that the concept of Open Radio Access Networks (Open RAN) has emerged as a potential path to drive 5G innovation by the United States, in turn providing opportunities for more secure networks, in addition to a host of other benefits.³ Some claim that the development and deployment of Open RAN could lead to benefits like greater vendor diversity, more flexible network architectures, lower capital and operating expenses, and new services tailored to unique use cases and consumer needs.⁴ Others contend that Open RAN is still in its most formative stages, that it will take months if not years to develop the software and protocols to achieve fully Open RAN-compliant end-to-end networks, and that traditional single-sourced networks provide the features, reliability, and security that networks need today.⁵

3. This Notice of Inquiry thus seeks comment on the status of Open RAN: where the technology is today, and what steps are required to deploy Open RAN networks broadly and at scale. In particular, this Notice of Inquiry seeks input on whether, and if so, how, deployment of Open RAN-compliant networks could further the Commission’s policy goals and statutory obligations, advance legislative priorities, and benefit American consumers by making state-of-the-art wireless broadband available faster and to more people in additional parts of the country.⁶ We undertake this timely inquiry

¹ 47 U.S.C. § 151.

² 47 U.S.C. § 157(a).

³ See, e.g., O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>.

⁴ *Id.*

⁵ Ericsson, *Security Considerations of Open RAN*, <https://www.ericsson.com/en/security/security-considerations-of-open-ran> (last visited Feb. 22, 2021).

⁶As discussed further below, the concept of virtualized RAN (vRAN), which utilizes open interfaces, is a component of some, but not necessarily all, types of Open RAN systems, and may be interoperable while still proprietary. To

(continued....)

at an important time for our nation's service providers. Many carriers are currently considering which equipment to deploy as they transition to 5G, and the Commission is also developing the Secure and Trusted Communications Networks Reimbursement Program to remove and replace insecure equipment and services from communications networks.⁷ The information developed in this Notice of Inquiry can inform carriers' decision-making as they examine which equipment and services to deploy in their next generation networks.

II. BACKGROUND

4. Open and virtualized radio access networks have the potential to address national security and other concerns that the Commission and other federal stakeholders have raised in recent years about network integrity and supply chain reliability. New startups are entering the original equipment manufacturer marketplace, and many of these companies are located in trusted-partner countries that do not pose national security risks. Network function virtualization and tools like artificial intelligence and machine learning (AI/ML) have the potential to allow for smarter, more efficient network security monitoring. Below, we summarize recent federal actions taken to help secure the communications supply chain and communications networks, either before the emergence of Open RAN or in parallel with these efforts.

A. Open RAN Development and Future Use

5. *Radio Access Network Architecture.* The RAN is the portion of the wireless telecommunication system that connects user devices (e.g., mobile phones) with the core network that performs routing or delivery of content. RAN architectures are wide-ranging in their degree of openness. For example, some vendors offer interoperable solutions that are proprietary but otherwise adhere to 3GPP standards, while other vendors purport to offer entirely open end-to-end network solutions or offer generic cloud-based or software-based neutral host services.⁸ Open RAN is a term that describes a general disaggregation of RAN functionality built using open interface specifications between elements instead of proprietary specifications. Open RAN can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards providing a flexible and interoperable deployment architecture across multiple vendors.⁹ Virtualized RAN (vRAN) is a term that refers to an implementation of the RAN which virtualizes network functions in software platforms based on general purpose processors.¹⁰ vRAN utilizing open interfaces is a component of some, but not necessarily all, types of Open RAN systems. Traditional RAN refers to traditional RAN architecture that leverages proprietary, embedded, fixed, and vertically integrated platforms.

6. Regardless of whether they are open, closed, or hybrid, the end-to-end RAN architectures are broadly based on specific components, arranged generally as shown in Figure 1 below. Briefly, these components can be described as follows (described in terms of the 3GPP standards, top-down):

- *Central Unit (CU):* oversees the radio resource control (RRC) and packet data convergence protocol layers of the network, controls multiple Distributed Units (DUs) over mid-haul interface, and facilitates network traffic load balancing among Radio Units (RUs);

the extent this Notice of Inquiry asks questions that reference Open RAN, we seek comment in equal measure on virtualized RAN where applicable.

⁷ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14330, para. 106 (2020) (*Supply Chain Second R&O*).

⁸ Federal Communications Commission, *Federal Communications Commission Technological Advisory Council Meeting*, June 4, 2020, <https://www.fcc.gov/sites/default/files/tac-presentations-6-4-20.pdf>.

⁹ Mavenir, *Understanding Open RAN*, <https://mavenir.com/portfolio/access-edge-solutions/radio-access/understanding-openran-5g/> (last visited Feb. 3, 2021).

¹⁰ *Id.*

- *Distributed Unit (DU)*: manages the radio link, data link, and digital portions of the physical layer of the network, and controls coordinated multi-point and fronthaul capabilities among multiple RUs;
- *Radio Unit (RU)*: consists of the digital front-end and the air-interface portions of the physical layer of the network.

7. The DU may be aggregated along with an RU or group of RUs. In either case, the control plane (CP) and the user plane (UP) of the CU are distinct and separate for security reasons.¹¹ In contrast, in an Open RAN architecture, open components are further broken down into functionally modularized subcomponents, each with standardized specifications for interfacing with other components to ensure interoperability, thus allowing a more diverse array of solutions to achieve equivalent network performance to more closed systems.

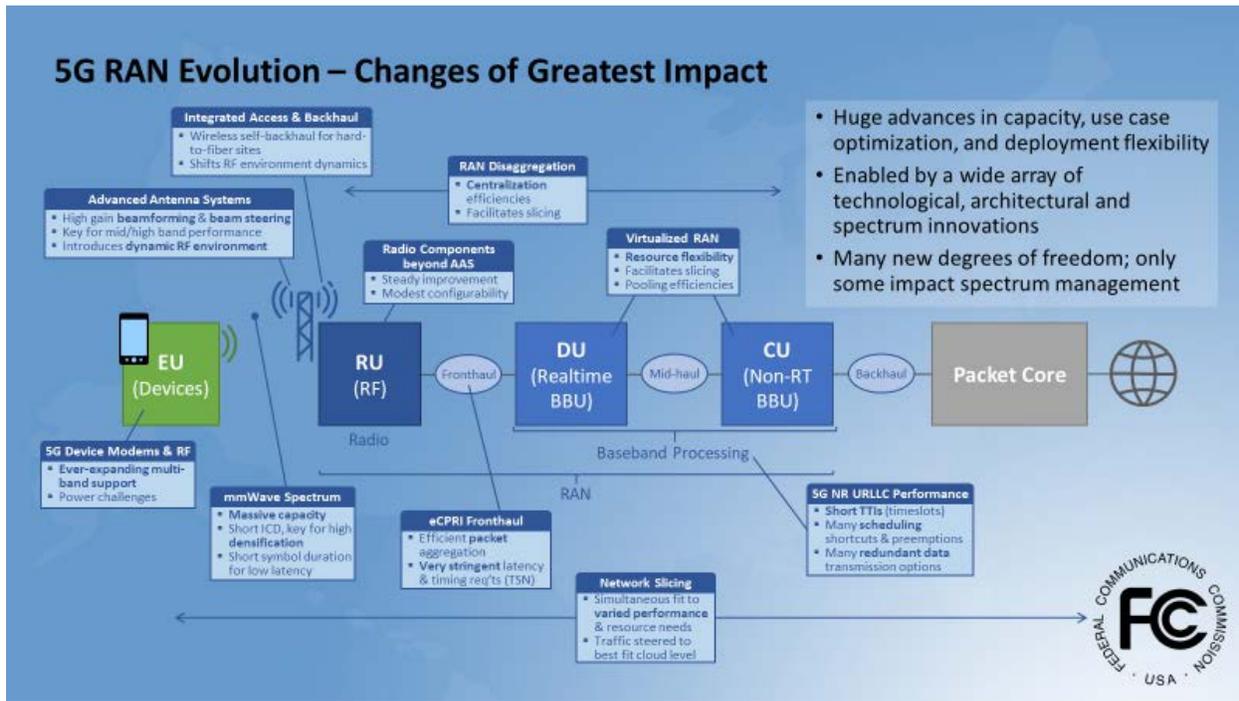


Figure 1. 5G RAN Evolution – Changes of Greatest Impact. Source: Federal Communications Commission, *Meeting of the Technological Advisory Council (TAC)* (Dec. 1, 2020), <https://www.fcc.gov/sites/default/files/tac-presentations-12-1-20.pdf>.

8. *Open RAN Architecture.* Open RAN architectures necessarily follow the same general architectures as traditional RAN architectures, including consistency between interfaces and technical specifications, and they use the same components (phones, base stations and transport medium) and the same technical standards as specified by 3GPP, the global industry standards organization for mobile technology.¹² However, Open RAN modularizes the hardware and software components of the traditional RAN to promote virtualization, to enable AI/ML solutions to optimize performance, and to enable interoperability across multiple vendors. Open RAN systems use an architecture capable of virtualization, with a goal of increased diversity of vendors and solutions.¹³ The systems can have components that are hardware-based or software-based, where the software may be open-source to

¹¹ See 3GPP, *Control and User Plane Separation of EPC Nodes (CUPS)* (July 3, 2017), <https://www.3gpp.org/cups>.

¹² 3GPP refers to the Third Generation Partnership Project, a consortium of telecommunication standards organizations responsible for developing protocols for mobile telecommunications, including LTE (4G) and 5G.

¹³ Fig. 1.

enhance innovation and interoperability. Certain components could also run on scalable cloud resources. The primary differences between the 3GPP architecture and the Open RAN architecture involve the disaggregation of the RAN Intelligent Controller (RIC) to separate near-real-time (near-RT) and non-real-time (non-RT) network services,¹⁴ and the clear distinction between DU and RU roles to facilitate openness, virtualization, and scalability of each of these components in the Open RAN architecture. These modifications to the architecture are intended to facilitate features such as cloud deployment, optimization of service provisioning, open mid-haul,¹⁵ and optimized quality of experience for each network user.¹⁶ The modifications also facilitate features such as low-cost, whitebox RAN hardware implementation, RAN sharing and slicing (*i.e.*, neutral host), and open fronthaul.¹⁷

9. Open initiatives exist at each architecture layer of the network. For instance, Open Network Automation Platform establishes a comprehensive platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers, and enterprises.¹⁸

10. The activity and interest in Open RAN is aimed at driving historically closed solutions to become more open and interoperable.¹⁹ Advances by 3GPP have enabled the development and adoption of Open RAN solutions. Previous RAN architectures (2G, 3G, and 4G) were based on monolithic building blocks, where most RAN components were supplied by a single vendor. Over the past decade, 3GPP has outlined and defined the RU, DU, and CU functional split, which enables components of the RAN to be interoperable with other third party DUs and RUs. The functional split development is a fundamental premise for Open RAN development, eliminating the need for a single supplier of the end-to-end system and providing the flexibility to deploy solutions tailored to unique use cases and consumer needs.

B. Recent U.S. Government Actions Related to Supply Chain and Network Security

1. Commission Orders and Actions

11. *Supply Chain Proceeding*. On November 22, 2019, the Commission adopted the *Supply Chain Order and Further Notice* to protect the communications supply chain against national security threats.²⁰ The *Order* adopted a rule, codified at 47 CFR § 54.9, that prohibits the use of universal service fund (USF) support to “purchase, maintain, improve, modify, operate, manage, or otherwise support any

¹⁴ See O-RAN Alliance, *O-RAN: Towards an Open and Smart RAN White Paper* at 10-11 (Oct. 2018) <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5bc79b371905f4197055e8c6/1539808057078/O-RAN+WP+Final+181017.pdf>. Non-RT control functionality (*i.e.*, required response times more than one second) includes service and policy management, RAN analytics, and model training. Near-RT control functions (*i.e.*, required response times less than one second) take trained models and real-time control functions produced in the non-RT RIC as input to the near-RT RIC for runtime execution.

¹⁵ See Fig. 1.

¹⁶ See O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 7 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>.

¹⁷ *Id.* at 20.

¹⁸ See The Linux Foundation, *Open Network Automation Platform*, <https://www.onap.org/> (last visited Feb. 3, 2021).

¹⁹ John Baker, *What is the Difference Between OpenRAN, O-RAN, and vRAN, Mavenir* (Mar. 20, 2020), <https://mavenir.com/blog/what-is-the-difference-between-openran-o-ran-and-vran/>

²⁰ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11433, para. 26 (2019) (*2019 Supply Chain Order or Supply Chain Order and Further Notice*), appeal pending in *Huawei Technologies USA v. FCC*, No. 19-60896 (5th Cir.).

equipment or services produced or provided by a covered company.”²¹ It also sets forth a process by which the Commission would designate a covered company that poses a threat to the integrity of communications networks and the communications supply chain,²² and prohibit the purchase of equipment or services produced or provided by that company. The Commission’s Public Safety and Homeland Security Bureau issued final designations on June 30, 2020, of both Huawei and ZTE as covered companies.²³ Pursuant to these designations, USF support may no longer be used to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by Huawei, ZTE, or any of the subsidiaries, parents, or affiliates of those two covered companies.

12. The *Supply Chain Order and Further Notice* also sought comment on a proposal to “require, as a condition on the receipt of any USF support that ETCs [eligible telecommunications carriers] not use or agree to not use within a designated period of time, communications equipment or services from covered companies.”²⁴ The Commission also proposed to establish a program to reimburse costs incurred by ETCs required to remove and replace covered equipment and services.²⁵ At the same time, the Commission adopted an *Information Collection Order*, which required ETCs to report whether they own or use Huawei or ZTE equipment or services in their networks and the cost of removing and replacing such equipment or services, to gauge the potential cost of this proposed reimbursement program.²⁶

13. On December 10, 2020, the Commission addressed in the *Supply Chain Second R&O* the 2019 proposals, as well as implementation of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act),²⁷ described in detail below.²⁸ The *Supply Chain Second R&O* established a rule requiring “recipients of reimbursement funds under the Reimbursement Program²⁹ and ETCs receiving USF support to remove and replace from their network and operations environments equipment and services included on the Covered List”³⁰ The Commission also enacted rules governing the

²¹ 47 CFR § 54.9.

²² *Supply Chain Order and Further Notice*, 34 FCC Rcd at 11438, para. 39.

²³ See generally *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*ZTE Designation Order*). See also *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Memorandum Opinion and Order, 35 FCC Rcd 14435 (PSHSB 2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 13146 (PSHSB 2020).

²⁴ *Supply Chain Order and Further Notice*, 34 FCC Rcd at 11470-71, para. 122.

²⁵ *Id.*

²⁶ *Id.* at 11481-82, paras. 162-63. The Wireline Competition Bureau released the results of this collection in September 2020. See *Wireline Competition Bureau and Office of Economics and Analytics Release Results from Supply Chain Security Information Collection*, WC Docket No. 18-89, Public Notice, DA 20-1037 (WCB Sep. 4, 2020) (*Information Collection Results PN*).

²⁷ Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609) (Secure Networks Act).

²⁸ See *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14290, para. 16 (2020) (*Supply Chain Second R&O*).

²⁹ The Secure and Trusted Communications Networks Reimbursement Program (Reimbursement Program) was created to facilitate the removal, replacement, and disposal of covered communications equipment and services.

³⁰ *Supply Chain Second R&O*, 35 FCC Rcd 14290, para. 18.

creation and maintenance of the Covered List to identify the communications equipment and services that pose an unacceptable risk to national security,³¹ created the Reimbursement Program,³² established a “Replacement List” of suggested replacements for the equipment and services being removed, replaced, and destroyed, and adopted an annual reporting requirement for all providers of advanced communications service to report covered communications equipment or services in their networks.³³

14. The *Supply Chain Second R&O* allowed the Replacement List to include Open RAN and virtualized network equipment, finding that doing so would be consistent with congressional intent and that such inclusion “could transform 5G network architecture, costs, and security.”³⁴ The Commission specifically encouraged Reimbursement Program participants to consider Open RAN, along with all other available technologies, as they make procurement decisions.³⁵

15. The Commission has promoted industry and public interest in Open RAN and other virtual network technologies in other fora as well. In 2010, the Commission formed the TAC, a group of industry representatives that provides technical advice to the Commission under the authority of the Federal Advisory Committee Act.³⁶ One of the TAC’s current four working groups studies vRAN as well as 5G technology and Internet of Things applications.³⁷ In December 2020, the working group recommended that the Commission encourage the development of the Open RAN ecosystem by supporting Open RAN innovation, standardization, testing, and security and reliability.³⁸ The TAC also recommended that the Commission support research and development opportunities related to Open RAN, including efforts related to open 5G/6G technologies and interoperability through public-private events such as “plugfests”³⁹ and testing in existing 5G testbeds.⁴⁰

16. In addition, the Commission’s Communications Security, Reliability, and Interoperability Council (CSRIC)⁴¹ plans to evaluate existing and future impediments to 5G Open RAN deployment and

³¹ *Id.*, 35 FCC Rcd at 14311, para. 57.

³² *Id.*, 35 FCC Rcd at 14330-52, paras. 106-96.

³³ *Id.*, 35 FCC Rcd at 14369, para. 212. The Commission defined “advanced communications service” for this purpose as “high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction.” 47 CFR § 1.50001(a); *Supply Chain Second R&O*, 35 FCC Rcd 14310-11, para. 55;

³⁴ *Supply Chain Second R&O*, 35 FCC Rcd 14366, para. 202.

³⁵ *Id.*, 35 FCC Rcd at 14369, paras. 197-202.

³⁶ 5 U.S.C. App.

³⁷ Federal Communications Commission, *2020 TAC Working Groups*, <https://www.fcc.gov/sites/default/files/fcc-tac-wrkgrp-charter.pdf> (last visited Feb. 22, 2021)

³⁸ Federal Communications Commission, *Federal Communications Commission Technological Advisory Council Meeting*, at 232 (Dec. 1, 2020), <https://www.fcc.gov/sites/default/files/tac-presentations-12-1-20.pdf>.

³⁹ The O-RAN Alliance has conducted several plugfests to demonstrate the functionality and multi-vendor interoperability of Open RAN network equipment. At these plugfests companies come together to deal with the interoperability and performance challenges of the Open RAN ecosystem. See O-RAN Alliance, *Second Global O-RAN Alliance Plugfest Demonstrates the Accelerated Readiness of Multi-vendor O-RAN Compliant Network Infrastructure*, <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5f88ac86a861db37b8f7df78/1602792591334/O-RAN-2020.10.15-PR-2nd-O-RAN-Plugfest-v1.0.pdf> (last visited Feb. 22, 2021).

⁴⁰ Federal Communications Commission, *Federal Communications Commission Technological Advisory Council Meeting* (Dec. 1, 2020) at 232, <https://www.fcc.gov/sites/default/files/tac-presentations-12-1-20.pdf>.

⁴¹ CSRIC is an advisory committee established to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. See Federal Communications

(continued....)

explore solutions to accelerate deployment. The CSRIC has previously considered security risks in emerging 5G networks,⁴² and now seeks to expand upon this work to include an examination of Open RAN technology. Further, the CSRIC will consider how the Commission can promote the goals of secure, open, and interoperable networks through its participation in organizations like 3GPP and the Alliance for Telecommunications Industry Solutions.

17. Most recently, in September 2020, the Commission hosted the 5G Open Radio Access Networks forum for government, industry, and academia stakeholders to discuss the status of Open RAN development, the benefits of deployment, and lessons from the field. The forum demonstrated that Open RAN technologies are showing great promise in the U.S. and around the world, and that the public and private sectors continue to seek out opportunities to collaborate and help encourage their development and deployment.⁴³

2. Recent Legislation

18. The Commission's ongoing work to secure communications networks has dovetailed with concurrent Congressional action. As early as 2012, Congress warned of the counterintelligence and national security threats posed by some of the world's largest vendors of traditional, vertically integrated telecommunications networking equipment.⁴⁴ Since then, Congress and the Commission have taken a number of targeted steps to safeguard America's critical communications infrastructure from potential security threats.⁴⁵

19. *Secure and Trusted Communications Networks Act of 2019*. In March 2020, Congress passed the Secure Networks Act, which enhanced and refined measures of the Commission's *Supply Chain Order and Further Notice*.⁴⁶ The Act mandated that the Commission publish by March 12, 2021 a "Covered List" of communications equipment and services that pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons."⁴⁷ It also prohibited the Commission from applying its program funds to support equipment or services on the Covered List.⁴⁸ In addition, the Act established the Secure and Trusted Communications Networks Reimbursement Program

Commission, *Communications, Security, Reliability, and Interoperability Council*, <https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0> (last visited February 12, 2021).

⁴² See Federal Communications Commission, Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0 (2018), <https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0> (CSRIC VI, WG 3 Final Report).

⁴³ Federal Communications Commission, *Forum on 5G Open Radio Access Networks* (Sept. 14, 2020), <https://www.fcc.gov/news-events/events/forum-5g-virtual-radio-access-networks>.

⁴⁴ In 2012, the House Permanent Select Committee on Intelligence released a bipartisan report assessing the counterintelligence and security threat posed by Chinese telecommunications companies operating in or providing equipment to customers in the United States. Permanent Select Committee on Intelligence, U.S. House of Representatives, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE at iv (Oct. 8, 2012), [https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20\(final\).pdf](https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huaweizte%20investigative%20report%20(final).pdf).

⁴⁵ See, e.g., *Protecting Against National Security Threat to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Notice of Proposed Rulemaking, 33 FCC Rcd 4058 (2018) (*2018 Supply Chain Notice*); *Supply Chain Order and Further Notice*, 34 FCC Rcd 11423; *Huawei Designation Order*, 35 FCC Rcd 6604; *ZTE Designation Order*, 35 FCC 6633 .

⁴⁶ Secure Networks Act, Pub. L. No. 116-124, 133 Stat. 158.

⁴⁷ 47 U.S.C. § 1601(b)(1).

⁴⁸ See *id.* § 1602(a)(1)(A)-(B); see also 47 CFR § 54.9 (prohibiting the use of USF funds, among other subsidies, to purchase, rent, or otherwise obtain insecure communications equipment or services.)

to facilitate the removal, replacement, and disposal of covered communications equipment and services, and tasked the Commission with creating a list of suggested replacement equipment and services.⁴⁹ It also required all providers of advanced communications services to report annually “regarding whether such provider has purchased, rented, leased, or otherwise obtained any covered communications equipment or service . . . ,”⁵⁰ granted the Commission enforcement powers, and created additional new penalties for noncompliance beyond those in the Communications Act of 1934 and Commission rules.⁵¹

20. *Consolidated Appropriations Act, 2021.* On December 27, 2020, the Consolidated Appropriations Act, 2021, funded the implementation of the Secure Networks Act, appropriating \$1.9 billion total with \$1.895 billion directed to the Reimbursement Program.⁵² The Consolidated Appropriations Act, 2021, also amended portions of the Secure Networks Act.⁵³ On February 17, 2021, the Commission adopted the *Supply Chain Third Further Notice of Proposed Rulemaking*, which proposed to amend Commission rules consistent with the amended language of the Secure Networks Act.⁵⁴

21. Other recent legislation supporting the development of secure 5G networks, including by supporting Open RAN development, include the Utilizing Strategic Allied Telecommunications Act⁵⁵ and the Secure 5G and Beyond Act of 2020.⁵⁶

3. Other Government Actions

22. Other major federal government actions to identify and mitigate risks and threats to national security posed by malicious actors include Executive Orders, task forces, and agency working groups.⁵⁷ These efforts recognize the potential benefits that open and interoperable networks could

⁴⁹ See 47 U.S.C. § 1603(d)(1)(A).

⁵⁰ See *id.* § 1604(a).

⁵¹ See *id.* § 1606.

⁵² Consolidated Appropriations Act, 2021, Pub. L. 116-260, H.R. 133, Div. N-Additional Coronavirus Response and Relief, Title IX-Broadband Internet access Service, §§ 901, 906, 134 Stat. 1182 (Dec. 27, 2020) (Consolidated Appropriations Act of 2021).

⁵³ *Id.*

⁵⁴ *Protecting Against National Security Threat to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Further Notice of Proposed Rulemaking, FCC 21-26 (Feb. 17, 2021).

⁵⁵ William M. Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 (Jan. 1, 2021) (National Defense Authorization Act or NDAA) (providing \$750 million to support research and development of alternatives to Huawei and ZTE).

⁵⁶ Secure 5G and Beyond Act of 2020, Pub. L. 116-129, 134 Stat. 223 (Mar. 23, 2020) (Secure 5G Act) (requiring the development a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in and to assist allies and strategic partners in maximizing the security of next generation mobile telecommunications).

⁵⁷ See Exec. Order No. 13800 § 2(b), 82 Fed. Reg. 22391, 22393, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017) (directing the Secretary of Homeland Security, in coordination with agency heads, to identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities, and to determine how best to support cybersecurity risk management efforts); Department of Homeland Security, Press Release, *DHS Announces ICT Supply Chain Risk Management Task Force Members* (Nov. 15, 2018), <https://www.dhs.gov/news/2018/11/15/dhs-announces-ict-supply-chain-risk-management-task-force-members> (convening a public-private partnership to examine and develop consensus recommendations to identify and manage global information and communications supply chain risk); National Counterintelligence and Security Center, *Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains* (Sept. 25, 2020), <https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf> (explaining Department of Defense strategic objective for supply chain security).

provide. For example, strategic innovation in the 5G marketplace could foster trusted 5G vendors,⁵⁸ and a broader emphasis on the potential for open interfaces could advance and sustain U.S. 5G leadership and innovation.⁵⁹ To streamline these efforts, the U.S. has collaborated with other countries and established interagency initiatives to encourage the consideration of Open RAN solutions internationally. For instance, several U.S. departments and agencies, including the Commission, were actively involved in the development of the Prague Proposals – a set of recommendations for the responsible development, deployment, and maintenance of 5G networks and future communication technologies – that emphasize the importance of open, interoperable, secure standards.⁶⁰ In addition, the U.S. Department of State has led international efforts to help focus global interest on the potential benefits of Open RAN.

III. DISCUSSION

A. State of Development and Deployment of Open RAN Solutions

23. *Current Standards and Specifications.* We seek comment on the current state of standards and specifications development for 5G and Open RAN. During the last few years, there has been a concerted effort among some organizations to advance the Open RAN model. For example, in 2016 and 2018, respectively, several companies launched the Telecom Infra Project (TIP) and global carriers established the O-RAN Alliance to develop and promote Open RAN reference architectures and protocols that foster vendor interoperability.⁶¹ In May 2020, several major global companies formed the Open RAN Policy Coalition to promote government policies that advance the adoption of open and interoperable RAN technologies.⁶² In August 2020, the Open Networking Foundation (ONF), an operator-led consortium advancing innovation in network infrastructure and carrier business models, announced several new initiatives in the Open RAN domain.⁶³ We seek comment on the state of Open

⁵⁸ U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, *CISA 5G STRATEGY: Ensuring the Security and Resilience of 5G Infrastructure In Our Nation* (2020), Strategic Initiative 4, https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

⁵⁹ NTIA, *National Strategy to Secure 5G Implementation Plan* (Jan. 19, 2021), <https://www.ntia.gov/5g-implementation-plan>.

⁶⁰ Prague 5G Security Conference, *The Prague Proposals: The Chairman statement on cyber security of communications networks in a globally digitized world* (May 3, 2019), https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf. The Commission played an active role in supporting U.S. efforts in the development of the Prague Proposals.

⁶¹ The TIP was founded by Deutsche Telekom, Intel, Facebook, Nokia, and SK Telecom. See Telecom Infra Project, *About TIP*, <https://telecominfraproject.com/faq/> (last visited Feb. 4, 2021). See also Deloitte, *The Next-Generation Radio Network: Open and Virtual RANs are the Future of Mobile Networks* (Dec. 7, 2020), <https://www2.deloitte.com/x/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/radio-access-networks.html/#endnote-1>. The O-RAN Alliance was formed jointly by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange. Technical workgroups within the O-RAN Alliance develop specifications and software for distinct components of the O-RAN Architecture, while focus groups address overarching O-RAN issues, such as standardization strategies, testing, and integration. See O-RAN Alliance, *About O-RAN Alliance*, <https://www.o-ran.org/about> (last visited Feb. 4, 2021); AT&T, *Industry Leaders Launch ORAN Alliance* (Feb. 27, 2018), https://about.att.com/story/industry_leaders_launch_oran_alliance.html.

⁶² Open RAN Policy Coalition, *Open RAN Policy Coalition Launches to Advance Open and Interoperable Solutions to Expand The Global Advanced Wireless Supply Chain*, <https://www.openranpolicy.org/open-fan-policy-coalition-launches-to-advance-open-and-interoperable-solutions-to-expand-the-global-advanced-wireless-supply-chain/> (last visited Feb. 4, 2021). In February 2020, the O-RAN Alliance and TIP announced an information-sharing liaison agreement to prevent duplication of effort, ensure alignment on O-RAN principles, and promote commercial O-RAN deployments. Fierce Wireless, *TIP, O-RAN Alliance Reach Liaison Agreement* (Feb. 25, 2020), <https://www.fiercewireless.com/wireless/tip-o-ran-alliance-reach-liaison-agreement>.

⁶³ Open Networking Foundation, *ONF Announces New 5G SD-RAN Project* (Aug. 25, 2020), <https://onfstaging1.opennetworking.org/news-and-events/press-releases/onf-announces-new-5g-sd-ran-project/>.

(continued....)

RAN standards development generally and, specifically, on the challenges inherent in developing Open RAN standards and specifications. To what extent are these standard-setting efforts being driven by established large manufacturers, and to what extent are these efforts enabling participation by smaller equipment vendors, smaller mobile network operators, and newer entrants to the marketplace? Are specifications such as eCPRI, the Common Public Radio Interface,⁶⁴ a sufficient alternative to Open RAN? Are there any known interoperable multivendor implementations of eCPRI? Are there substantive differences between the eCPRI and Open RAN approaches for disaggregating the network? What steps, if any, should be taken by the Commission to help resolve standard-setting challenges, bolster these efforts, and accelerate the timeline for Open RAN standards and specifications development?

24. *Open RAN Ecosystem.* We seek comment on the current state of the Open RAN ecosystem. For example, which companies are offering baseband hardware, network virtualization, packet core functionality, or other network components? How large are each of these companies, in sales or revenues, in each of these applications? How scalable is manufacturing of each of these components to allow for ramp up in production? And how many companies are competing to supply each of the components and applications? What role (if any) will systems integrators play in advancing the deployment of Open RAN systems and what systems integrators are operating in the marketplace today? Will carriers execute their own integration, as Rakuten has done, or buy hosted solutions from other providers?⁶⁵ Commenters should identify any gaps or potential bottlenecks in the Open RAN ecosystem. What factors incentivize or disincentivize vendors from developing Open RAN solutions? What are the financial capabilities and funding sources of current or potential vendors to develop such solutions? To what extent does the development of Open RAN solutions by one firm depend on the development of Open RAN by other firms?

25. We seek comment on the current and future opportunities that Open RAN generates for the U.S. wireless infrastructure industry. While U.S. companies do not currently offer an integrated end-to-end network at scale, several companies compete for various components of the network.⁶⁶ Does this suggest that U.S. companies are well positioned to compete in a modular market? More specifically, we seek comment and data on whether and, if so, how many U.S. companies or vendors can manufacture and/or supply Open RAN sub-components, including radios, at the scale necessary to compete both domestically and internationally with traditional network equipment vendors. How many U.S. companies have the knowledge and resources to begin manufacturing Open RAN components and applications in the near future? What are the projected market shares of the U.S. companies at the aggregate level in the U.S. wireless network equipment market if Open RAN were widely adopted? Are there any components or applications for which there currently are no U.S. suppliers?

ONF launched, for example, the Software Defined Radio Access Network (SD-RAN) project to create open-source platforms compatible with the O-RAN architecture. The O-RAN Alliance formed a similar information sharing arrangement with ONF in January 2020. Open Networking Foundation, *ONF Working with O-RAN Alliance* (Jan. 17, 2020), <https://opennetworking.org/uncategorized/onf-working-with-o-ran-alliance/>.

⁶⁴ See Ericsson AB, Huawei Technologies Co, Ltd, NEC Corporation, and Nokia, *Common Public Radio Interface: eCPRI Interface Specification V2.0*, (May 10, 2019), http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf.

⁶⁵ See Mike Dano, *Rakuten to sell mobile platform globally, likely targeting Dish*, Light Reading (March 18, 2020), <https://www.lightreading.com/ai-automation/rakuten-to-sell-mobile-platform-globally-likely-targeting-dish/d/d-id/758282>.

⁶⁶ See, e.g., Melissa K. Griffith, Wilson Center, *Open RAN and 5G: Looking Beyond the National Security Hype*, (Nov. 2, 2020), <https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype> (noting that U.S. vendors are among the market leaders in end-user devices (Apple, Cisco, and Qualcomm) and the core network (Cisco and Juniper)); see also James Andrew Lewis, Center for Strategic and International Studies, *How 5G Will Shape Innovation and Security*, (Dec. 6, 2018), <https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security> (emphasizing that semiconductors are the most important components of 5G technologies and American companies are still the major suppliers).

26. *Domestic Deployments.* We seek comment on the current state of Open RAN deployments in the U.S. To what extent are these solutions commercially available today? While DISH has not announced a launch date,⁶⁷ it is currently building the first nationwide cloud-native, Open RAN-based 5G broadband network.⁶⁸ Inland Cellular, a rural mobile wireless service provider that serves more than 35,000 subscribers in Idaho and Washington, is reportedly deploying an Open RAN system that will cut per site cost by approximately 40 percent.⁶⁹ Verizon Wireless has reportedly deployed vRAN equipment as part of its 5G network.⁷⁰ What other U.S. companies are planning or otherwise participating in Open RAN deployments? How close is the U.S. to being ready for large-scale deployments? Has Open RAN delivered an integrated and truly interoperable end-to-end process in the United States yet? Commenters should discuss previous and current efforts to deploy Open RAN in the U.S., as well as any expected plans to deploy in the future, including information on the costs of any deployments considered. We seek comment on which mobile network operators or original equipment manufacturers are likely and not likely to adopt Open RAN. What factors are preventing, impeding, or discouraging Open RAN deployments? What steps should be taken by the Commission, other federal partners, industry, academia, or others to resolve these issues, address these concerns, and accelerate the timeline for Open RAN deployment?

27. *International Deployments.* Similarly to the United States, several countries have stressed the importance of securing their communications networks and communications supply chains. The United Kingdom has established a 5G Supply Chain Diversification Strategy to ensure the telecom supply chain remains resilient to future trends and threats,⁷¹ and French suppliers are being prioritized to help the French government reduce its dependence on Huawei.⁷² Several countries believe that Open RAN can offer a solution to security issues affecting the communications network supply chain. The German government, for example, is expected to spend 2 billion euros to reduce dependency on Huawei and to prioritize Open RAN research, development, deployments.⁷³

⁶⁷ DISH committed to the Commission that if it did not deploy a nationwide 5G network covering at least 70 percent of the population by June 2023, it would pay up to \$2 billion in fines and divest up to \$12 billion worth of spectrum. See *Applications of T-Mobile US, Inc., and Sprint Corp. for Consent to Transfer Control of Licenses and Authorizations*, WT Docket No. 18-197, Order, 35 FCC Rcd 9580, 9586, para. 12 (2020); see also *New York v. Deutsche Telekom AG*, 439 F. Supp. 3d 179, 198 (S.D.N.Y. Feb. 11, 2020); DISH, *DISH to Become National Facilities-Based Wireless Carrier* (July 26, 2019), <https://ir.dish.com/news-releases/news-release-details/dish-become-national-facilities-based-wireless-carrier>.

⁶⁸ DISH, *DISH Advances O-RAN Network, Selects Fujitsu for 5G Radio Units and Altiostar for Virtualized RAN Software Solution* (June 30, 2020), <https://about.dish.com/2020-06-30-DISH-advances-O-RAN-network-Selects-Fujitsu-for-5G-radio-units-and-Altiostar-for-virtualized-RAN-software-solution>.

⁶⁹ See Sean Kinney, RCR Wireless, *Inland Cellular Using OpenRAN in Idaho* (June 30, 2020), https://www.rcrwireless.com/20200630/open_ran/inland-cellular-using-openran-in-idaho; see also Jeanne Whalen, Washington Post, *A remote corner of Idaho has become the best hope for the U.S. challenge to Huawei*, (June 29, 2020), <https://www.washingtonpost.com/business/2020/06/29/huawei-alternative-oran-idaho/>.

⁷⁰ See Bevin Fletcher, Fierce Wireless, *Verizon deploys Samsung vRAN in 5G expansion*, (Jan. 22, 2021), <https://www.fiercewireless.com/5g/verizon-deploys-vran-from-samsung-for-5g-expansion>.

⁷¹ See UK Department for Digital, Culture, Media and Sport, *5G Supply Chain Diversification Strategy* (Dec. 7, 2020), <https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy>.

⁷² See Press Release, NASDAQ, *Sequans Receives Major Funding Award for 5G Development from French Government* (Jan. 28, 2021), <https://www.nasdaq.com/press-release/sequans-receives-major-funding-award-for-5g-development-from-french-government-2021>.

⁷³ See Ray Le Maistre, TelecomTV, *Open RAN Projects in Line for Massive German Government Funds: Report*, (Jan. 22, 2021), <https://www.telecomtv.com/content/open-ran/open-ran-projects-in-line-for-massive-german-government-funds-report-40682/>.

28. In response to government policies and demand for more secure solutions, operators worldwide are developing and deploying Open RAN architectures at an increasing rate. For example, in Asia, Rakuten claims it was one of the first companies to utilize Open RAN as part of their new fully virtualized cloud network in Japan,⁷⁴ and Bharti Airtel and Vodafone Idea have been at the forefront of Open RAN deployments in India.⁷⁵ In Europe, four major carriers – Vodafone Group Plc, Telefonica S.A., Deutsche Telekom AG, and Orange S.A. – signed a Memorandum of Understanding signaling their commitment to deploy Open RAN solutions across Europe.⁷⁶ In Africa, Vodafone has conducted early field trials,⁷⁷ and Orange announced in July 2020 a multi-country program to extend their current coverage with Open RAN solutions, including in the Central African Republic.⁷⁸ In Latin America, the TIP, Instituto Nacional de Telecomunicaciones (Inatel) and Telecom Italia Mobile (TIM) Brasil launched the Open Field program in Brazil to develop and test Open RAN solutions in the field.⁷⁹

29. As countries and operators worldwide are beginning to coalesce around the Open RAN model, we seek comment on what lessons can be learned from successful deployments, previous failed deployments, and development efforts being undertaken in other countries. What has been learned about deploying Open RAN systems using existing generations of networks and in low-income and rural environments? What challenges have these operators faced in developing and deploying Open RAN systems? Is there anything about the U.S. wireless network industry, spectrum policies (e.g., availability of greenfield spectrum), or geographical or other factors that present unique challenges to Open RAN deployment? What steps can the Commission take to encourage timely and secure domestic deployments? What implications do international efforts like the European Memorandum of

⁷⁴ See Press Release, Rakuten, *Rakuten Mobile Launches 5G Service with New Plan, Same Monthly Fee: Rakuten UN-LIMIT V* (Sep. 30, 2020), https://global.rakuten.com/corp/news/press/2020/0930_02.html.

⁷⁵ Press Release, Altiostar, *Bharti Airtel Deploys Open vRAN with Altiostar* (April 29, 2020), <https://www.altiostar.com/bharti-airtel-deploys-open-vran-with-altiostar/>; Press Release, Mavenir, *Vodafone Idea Deploys Mavenir OpenRAN Solution* (April 23, 2020), <https://mavenir.com/press-releases/vodafone-idea-deploys-mavenir-openran-solution/>.

⁷⁶ GSM Association, *Major European Operators Sign Open RAN MOU* (Jan. 26, 2021), <https://www.gsma.com/futurenetworks/digest/major-european-operators-sign-open-ran-mou/>; Press Release, Orange, *Major European Operators Commit to Open RAN Deployments* (Jan. 20, 2021), <https://www.orange.com/en/newsroom/press-releases/2021/major-european-operators-commit-open-ran-deployments>. In Germany, Telefónica became the first German supplier to rely on O-RAN for its live mobile network. Press Release, Telefónica, *First German Network Operator with Open RAN in Live Operation* (Dec. 15, 2020), <https://www.telefonica.de/news/press-releases-telefonica-germany/2020/12/telefonica-o2-first-german-network-operator-with-open-ran-in-live-operation.html>. Deutsche Telekom has also made significant investments in O-RAN deployment and is working on “O-RAN Town.” See TelecomTV, *Deutsche Telekom Preps 2021 Open RAN Rollout* (Dec. 10, 2020), <https://www.telecomtv.com/content/open-ran/deutsche-telekom-preps-2021-open-ran-rollout-40429/>.

⁷⁷ Press Release, Vodafone, *Vodafone Pioneers Innovative Network Tech to Increase Suppliers and Extend Rural Internet Access* (Oct. 7, 2019), <https://www.vodafone.com/news/press-release/vodafone-pioneers-innovative-network-tech-to-increase-suppliers-and-extend-rural-internet-access>.

⁷⁸ Press Release, PR Newswire, *Parallel Wireless Helps to Deliver on Orange’s Open RAN Vision in Central African Republic* (July 16, 2020), <https://www.prnewswire.com/news-releases/parallel-wireless-helps-to-deliver-on-oranges-open-ran-vision-in-central-african-republic-301092745.html>.

⁷⁹ Press Release, Telecom Infra Project, *TIP Community Achieving Significant Momentum on the Path to Open, Interoperable, Disaggregated and Standards-based Networks* (Oct. 6, 2020), <https://telecominfraproject.com/tip-community-achieving-significant-momentum-on-the-path-to-open-interoperable-disaggregated-and-standards-based-networks/>.

Understanding⁸⁰ have for U.S. leadership in this area?

B. Potential Public Interest Benefits in Promoting Development and Deployment of Open RAN

1. Increased Competition and Network Vendor Diversity

30. We seek comment generally on the effect of Open RAN on market entry, vendor diversity, and competition in the wireless network equipment industry. We seek comment on the current state of competition in the wireless network equipment industry generally and in the markets for various components and applications. What are the effects of competition in the industry, and would transitioning to Open RAN resolve, ameliorate, or worsen these issues? Specifically, would increased competition in the wireless network equipment marketplace result in lower costs for operators? Commenters advocating this position should explain why and should estimate the likely cost reductions. For instance, does Open RAN eliminate or minimize the costs associated with developing a proprietary end-to-end network or deploying and maintaining single-vendor hardware? What benefits can be gained by access to interoperable networks? On the other hand, would there be any additional costs to operators from having to use Open RAN versus alternative technologies? For example, are there any additional costs required for integrating the Open RAN system?

31. We also seek this information on the firms that supply various network components and applications of 5G RAN networks and their market shares in each of the segments. We seek comment on the relationships between and among firms in this industry, including but not limited to supplier relationships, equity investments, and joint ventures or partnerships. Commenters should also describe the extent to which the cost, quality, and/or capabilities of competing components and applications differ.

32. We seek comment on the current and projected demand for Open RAN and its expected market share, as a proxy for predicting the level of competition in the Open RAN supply chain. By some estimates, Open RAN currently captures 9.4% of the total 4G and 5G market.⁸¹ Is the current market share a reflection of actual demand, or is it the result of regulatory or other barriers that may be impeding or delaying widespread adoption and deployment? Is market share likely to change in the future? Is there a threshold for market share at which the effectiveness of diffusion of Open RAN would rapidly increase? What are the anticipated diffusion rates over the next 5 years under current market conditions? We seek comment on whether the pace of Open RAN adoption should influence policies the Commission adopts, or whether the Commission should adopt policies to accelerate the pace of adoption. We also seek comment on any adverse effects and costs of policies advocated by commenters, such as the extra burden on network operations that the policies may cause.

33. What factors may incentivize or disincentivize operators from adopting Open RAN technologies? How would adoption by one firm impact adoption by other firms? To what extent does Open RAN technology exhibit economies of scale, network effects, or learning curves? To what extent might government-funded incentives or other regulatory intervention ease any of the costs or barriers to adopting Open RAN? For example, the Indian government is currently drafting procurement regulations for its next generation networks and is expected to offer preference to domestic suppliers.⁸² In Japan, the

⁸⁰ Memorandum of Understanding on the Implementation of OPEN RAN based Networks in Europe (Jan. 18, 2021), <https://www.orange.com/sites/orange.com/files/2021-01/Memorandum%20of%20Understanding%20OPEN%20RAN.PDF>.

⁸¹ Ian Morris, Light Reading, *Open RAN Will Be A \$3.2B Market in 2024, says Omdia* (Dec. 4, 2020), [https://www.lightreading.com/open-ran/open-ran-will-be-\\$32b-market-in-2024-says-omdia/d/d-id/765889](https://www.lightreading.com/open-ran/open-ran-will-be-$32b-market-in-2024-says-omdia/d/d-id/765889).

⁸² Kiran Rathee, The Indian Express, *TRAI Chairman: 'Open RAN Will Present Opportunities'* (Jan. 20, 2021), <https://indianexpress.com/article/business/trai-chairman-open-ran-will-present-opportunities-7153590/>.

government is providing tax incentives to products with open and interoperable interfaces,⁸³ and the UK government announced a 28 million euro investment in 5G products, with more than one-half utilizing Open RAN.⁸⁴ Should we adopt similar regulatory measures or incentives? If the benefits of Open RAN can only be realized by economies of scale, should the Commission provide funding or incentives to operators that choose to implement such systems in their wireless networks? Are other actions necessary to level the playing field for new Open RAN suppliers that are competing against entrenched traditional vendors with decades of experience? For instance, should we amend, forbear from applying, or eliminate any of our rules that inadvertently support a single-vendor approach, a specific technology (e.g., closed radio access networks), or otherwise inhibit the development and adoption of Open RAN solutions? Are there any components or factors of an Open RAN system that are or could be hindered by a single or limited vendor supply? How can we facilitate a competitive marketplace where essential pieces of an Open RAN architecture aren't controlled by a limited number of entities?

34. We seek comment on whether Open RAN is likely to create opportunities for new entrants in the original equipment manufacturer markets. Specifically, we seek comment on whether, and if so which aspects of, the Open RAN architecture promote vendor diversity and competition. Open RAN works by disaggregating software applications from the underlying hardware infrastructure and replacing proprietary interfaces between baseband components with open, standards-based interfaces. Would the disaggregated nature of Open RAN lower the costs of entry by allowing vendors to develop distinct components of the network (e.g., hardware, software, silicon), rather than having to build the integrated end-to-end system, which can be a costly undertaking? Does the interoperable nature of Open RAN facilitate market entry by allowing vendors to develop specific components of the network for use by multiple operators rather than creating unique one-off solutions for specific operators? What specific firms or what kind of firms would be likely entrants, and how are they likely to perform as competitors against incumbents? Which segments are they likely to enter, and what kind of products are they likely to develop? Are there likely to be international entrants in addition to domestic entrants? Commenters should discuss other aspects of the Open RAN architecture that may lower the barriers to entry and otherwise facilitate market entry.

35. We also seek comment on how open access could encourage innovation by American companies, and how to anticipate, identify, and evaluate potential issues that might stifle innovation, manufacturing, and deployment. For example, is there a sufficient workforce in place with the training to safely and efficiently install Open RAN equipment? If not, how quickly could such workers be trained? Are there steps the Commission or other federal agencies should take to address an increase in the supply of trained workers needed to close such a gap? Under an open-source or open-interface model, will businesses be able to stay financially viable? How will access to intellectual property and patents influence the ability to innovate? Can U.S. operators continue to achieve the same level of features and performance at scale with Open RAN that customers currently enjoy with existing infrastructure? Will technological developments in Open RAN benefit innovation in other technologies? We seek comment on these questions as well as comment generally on whether the Commission or other entities could or should plan for and mitigate foreseeable roadblocks.

2. Affordability of Services and Products for Consumers

36. We seek comment on the potential costs and benefits of Open RAN on consumers in the next-generation wireless network marketplace. If Open RAN lowers the overall hardware and deployment costs for operators, are those cost savings likely to pass through to consumers in the form of lower, more competitive prices for next-generation wireless services? How might Open RAN affect the price of services and products for consumers, if at all? If the federal government provides incentives for a

⁸³ Mihoko Matsubara, Lawfare Blog, *Japan's 5G Approach Sets a Model for Global Cooperation* (Sept. 14, 2020), <https://www.lawfareblog.com/japans-5g-approach-sets-model-global-cooperation>.

⁸⁴ Ray Le Maistre, TelecomTV, *Open RAN Architectures at Heart of UK 5G Projects* (Jan. 18, 2021), <https://www.telecomtv.com/content/open-ran/open-ran-architectures-at-heart-of-uk-5g-projects-40645/>.

transition in architecture, how can we ensure these cost savings find their way to the consumer? Commenters should discuss the potential effect of Open RAN on the affordability of end-user services and products.

3. Network Security and Public Safety

37. Several countries have recognized Open RAN as a potential solution to the increasing security threats posed to their nation's communications supply chains. For example, as previously discussed, the German government is expected to spend two billion euros to reduce its dependency on Huawei by prioritizing Open RAN research and development and deployments.⁸⁵ France has adopted a similar policy.⁸⁶ Through open disaggregation of the RAN, Open RAN is intended to enable the use of interchangeable modular technologies, as well as AI/ML, to promote, among other things, network security and public safety. O-RAN Alliance argues that the design of Open RAN, along with the potential for leveraging open-source software, should improve supply chain security.⁸⁷

38. To what extent does Open RAN address supply chain risk management issues and enable the deployment of secure and reliable networks in the United States? Does the disaggregated nature of Open RAN facilitate market entry by additional vendors and therefore offer viable alternatives to the use of equipment from untrusted vendors in the telecommunications supply chain (e.g., Huawei and ZTE)?⁸⁸ Would Open RAN mitigate operators' reliance on specific vendors, allowing them to secure a back-up supplier or otherwise eliminate lock-in problems resulting from a consolidated equipment marketplace? How would an increase in the number of vendors supplying components for Open RAN affect the 5G vendor management ecosystem? Would the use of Open RAN software facilitate the rapid removal of vendors' equipment when they were identified as untrusted? Would a supply chain of Open RAN software vendors that excludes untrusted entities obviate concerns of that software running over hardware of an untrusted vendor? Can additional criteria be defined to assist in identifying what is an untrusted vendor, beyond frameworks such as the Prague Proposals,⁸⁹ EU Toolbox for 5G Security,⁹⁰ or the Center for Strategic and International Studies Criteria?⁹¹ We seek information on the risk of security breaches, including the frequency of such breaches and the magnitude of potential economic damages on closed RAN networks, and how this security risk could be addressed by Open RAN networks.

39. We seek comment on the potential impact of Open RAN on public safety communications. What potential benefits would Open RAN provide for public safety communications and emergency communications, such as 911 or wireless emergency alerting overall? To what extent

⁸⁵ Ray Le Maistre, TelecomTV, *Open RAN Projects in Line for Massive German Government Funds: Report* (Jan. 22, 2021), <https://www.telecomtv.com/content/open-ran/open-ran-projects-in-line-for-massive-german-government-funds-report-40682/>.

⁸⁶ See Press Release, NASDAQ, *Sequans Receives Major Funding Award for 5G Development from French Government* (Jan. 28, 2021), <https://www.nasdaq.com/press-release/sequans-receives-major-funding-award-for-5g-development-from-french-government-2021>.

⁸⁷ See e.g., O-RAN Alliance, *The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Components*, <https://www.o-ran.org/blog/2020/10/24/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components> (last accessed Feb. 11, 2021).

⁸⁸ See generally *ZTE Designation Order*; *Huawei Designation Order*.

⁸⁹ See Government of the Czech Republic, *The Prague Proposals*, <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>.

⁹⁰ See European Commission, *The EU toolbox for 5G security*, (Jan. 29, 2020), <https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security>.

⁹¹ See Center for Strategic & 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>.

would Open RAN impact the required location accuracy of 911 calls? How and to what extent would Open RAN facilitate interoperability for public safety communications, especially as state and local 911 systems transition to IP-based networks, such as Next Generation 911 (NG 911)? Similarly, how would Open RAN enhance interoperability with respect to NG 911, the First Responder Network (FirstNet), or priority services, such as wireless priority services? How could Open RAN reduce the overall frequency and duration of communications outages on networks that carry 911 and other emergency communications?

40. *Open-Source Software.* Open-source software “includes operating systems, applications, and programs in which the source code is published and made available to the public, enabling anyone to copy, modify and redistribute that code.”⁹² Open RAN can leverage open-source software for network functions and to manage the network. Open-source software draws from a larger and more diverse set of reviewers compared to that of a closed RAN architecture.⁹³ What are the potential benefits or advantages associated with the use of open-source software in Open RAN environments? For instance, does open-source software result in a well-vetted, more secure finished product? How can these benefits be most effectively realized, and what role can the Commission play in maximizing these benefits? What are the disadvantages to using open-source software in Open RAN environments and how can they be mitigated?

4. Potential Technological Benefits of Open RAN Deployment

41. Proponents of Open RAN argue that features such as end-to-end network slicing, edge computing, and machine learning-based network optimization methods may be better enabled by standards-based architectures.⁹⁴ Further, they contend that an open architecture could improve the controllability and overall performance of cellular networks that are increasingly heterogenous and distributed, aggregate spectrum in different frequency bands, and use small-cell architectures.⁹⁵ We seek comment on these views, and specifically on quantifying the improvement in spectral efficiency and performance under the Open RAN architecture as compared with a closed system.

42. One of the promised benefits of an Open RAN architecture is the ability to apply AI/ML techniques to optimizing radio resource management, since the interfaces between different elements of the network will be available for real-time control.⁹⁶ Proponents argue this would be especially beneficial in network slicing to guarantee end-to-end Quality-of-Service to disparate applications that are allocated

⁹² See Final Report – Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0, Communications Security, Reliability, and Interoperability Council (CSRIC Report) at 7,1 (2018), <https://www.fcc.gov/file/14500/download>.

⁹³ See Federal Communications Commission, Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards at § 5.11 (2020), <https://www.fcc.gov/files/csric7reportriskintroducedby3gpppdf> (CSRIC VII, WG 3 Final Report).

⁹⁴ See generally, 5G Americas, Transition Toward Open and Interoperable Networks White Paper at 7, 38 (Nov. 2020), <https://www.5gamericas.org/wp-content/uploads/2020/11/InDesign-Transition-Toward-Open-Interoperable-Networks-2020.pdf>; Telecom Infra Project, *OpenRAN Begins Work on AI/ML Applications for Radio Management* (July 28, 2020), <https://telecominfraproject.com/openran-begins-work-on-ai-ml-applications-for-radio-management/>.

⁹⁵ See generally, O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 7-8 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>.

⁹⁶ See, e.g., O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 9 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>; Telecom Infra Project, *OpenRAN Begins Work on AI/ML Applications for Radio Management* (July 28, 2020), <https://telecominfraproject.com/openran-begins-work-on-ai-ml-applications-for-radio-management/>.

resources over the network.⁹⁷ The complexity of wireless networks makes manual control and optimization inefficient, leading to wasted resources along multiple axes – spectrum, computing and infrastructure.⁹⁸ Open RAN proponents claim that AI/ML algorithms are increasingly being used even in the current RAN, and that an Open RAN architecture may enable improved performance by offering improved visibility to intermediate nodes within the RAN.⁹⁹

43. Advanced wireless networks, including 5G, may be used for “vertical” applications outside of traditional telecommunications networking, such as smart cities, automotive, telehealth, and energy. The network slicing and other features of an Open RAN architecture could better enable very different application suites to run on the same hardware stack. We seek comment on the benefits outlined above and what role the Commission should play in facilitating these benefits. We also seek comment on the status and viability of these benefits and ask commenters to quantify the value of such benefits. Are they available now, and if not, how long until the various benefits outlined above become viable? Are these benefits primarily (or exclusively) the result of Open RAN architecture or will they also result from 5G or other advanced wireless networks deployed using traditional network equipment? What are the potential obstacles or disadvantages of the technologies and approaches discussed above?

44. Radiofrequency spectrum is anticipated to be a key enabler for a variety of public ecosystems including aviation, marine, and land-based transportation infrastructure. Private sector initiatives are being organized that focus on advancing 5G innovation, such as MITRE Engenuity, which has created the Open Generation Consortium to drive 5G innovation, with an initial focus on 5G-equipped drones.¹⁰⁰ The advancement of 5G use cases for drones and other applications may face technological and regulatory barriers, and we seek comment on the barriers to the emerging ecosystem of Unmanned Aircraft Systems (UASs) as it relates to network equipment and architecture. MITRE suggested at the FCC’s September 2020 Forum on 5G Open Radio Access Networks that the UAS industry could be an attractive focus for Open RAN. Furthermore, the TAC has recommended a pilot program focused on the

⁹⁷ See, e.g., 5G Americas, *Transition Toward Open and Interoperable Networks White Paper* (Nov. 2020), <https://www.5gamericas.org/wp-content/uploads/2020/11/InDesign-Transition-Toward-Open-Interoperable-Networks-2020.pdf> at 35; O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 7 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>.

⁹⁸ See, e.g., O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 8-9 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>; Leonardo Bonati et al., *CellOS: Zero-Touch Softwarized Open Cellular Networks* (Oct. 24, 2020), <https://www.sciencedirect.com/science/article/pii/S138912862030503X>.

⁹⁹ See generally, Telecom Infra Project, *OpenRAN Begins Work on AI/ML Applications for Radio Management* (July 28, 2020), <https://telecominfraproject.com/openran-begins-work-on-ai-ml-applications-for-radio-management/>; 5G Americas, *Transition Toward Open and Interoperable Networks White Paper* (Nov. 2020), <https://www.5gamericas.org/wp-content/uploads/2020/11/InDesign-Transition-Toward-Open-Interoperable-Networks-2020.pdf> at 45; O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 9 (Feb. 2020), <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>; Rysavy, *Global 5G: Implications of a Transformational Technology* (Sept. 2019), <https://www.5gamericas.org/wp-content/uploads/2019/09/2019-5G-Americas-Rysavy-Implications-of-a-Transformational-Technology-White-Paper.pdf>.

¹⁰⁰ Mitre, *Mitre Engenuity Launches Open Generation Consortium to Drive 5G Innovation* (Nov. 10, 2020), <https://www.mitre.org/news/in-the-news/mitre-engenuity-launches-open-generation-consortium-to-drive-5g-innovation>.

evolving UAS use case.¹⁰¹ We seek comment on what network architecture issues need to be addressed to meet these challenges and how we might address any such challenges. We seek comment on this topic generally and, in particular, on the steps that the Commission could take to promote and advance the application of 5G Open RAN to the emerging UAS ecosystem.

45. *Artificial Intelligence and Machine Learning*. Using Open RAN may also enable providers to take advantage of AI and ML from sources other than a proprietary RAN vendor. The O-RAN Alliance contends that AI and ML enable the optimization of RAN configurations in real-time based on learning technologies that accumulate information over time.¹⁰² We seek comment on what steps industry, the Commission, or other organizations can take to promote the development and use of AI and ML to support and enhance the security features of an Open RAN deployment. Can AI and ML be harnessed to identify and remediate malicious changes in configuration or otherwise detect intrusions and vulnerabilities in an Open RAN platform? Are additional standards and Application Layer Interfaces (API) needed to ensure the development of security-based AI/ML features in Open RAN technologies? What other benefits and challenges exist regarding the use of AI and ML in our communications infrastructure and how do we balance those with potential privacy issues?

46. *Virtualized Operating Environment*. Proponents argue that Open RAN's use of virtualized environments with containers offers additional operational and security advantages.¹⁰³ Software virtualization could enable applications and operating environments to be isolated from each other. Containerization could allow multiple vendors to develop their products for the same Open RAN platform, and could encourage competition between vendors, thus driving down costs for the provider. Are there other advantages of virtualization in the context of security (e.g., data privacy, or protection of computer resources assigned to an Open RAN application)? What are the disadvantages and can they be addressed? We note that the Distributed Management Task Force is a standards body focusing on emerging IT infrastructures like cloud computing and virtualization. Are additional industry standards needed to facilitate various virtualization platforms for different hardware used to support Open RAN functionality and security?

C. Additional Considerations Regarding Open RAN Development and Deployment

1. Disaggregation/Need for a System Integrator

47. If the flexibility created by disaggregation of the RAN has potential benefits, would it also make the deployment of the Open RAN more complex than deployment of a closed RAN because different components must be seamlessly integrated? Since the different Open RAN components may be supplied by different vendors, how would operators resolve compatibility problems that arise during deployment, in spite of standardized interfaces being specified?

48. We seek information on the practical implications of the disaggregation of the components of the RAN. How difficult will it be to ensure that the components of the Open RAN seamlessly operate together? Will testing of the Open RAN deployment be a time-consuming and complicated process compared to a proprietary RAN? Have Open RAN deployments to date had comparable performance to 4G and 5G systems employing a traditional RAN architecture? Is the performance of Open RAN systems likely to be impacted due to the multi-vendor environment? Will

¹⁰¹ Federal Communications Commission, The Importance of Artificial Intelligence and Data for the Telecommunications Industry and the FCC, Report of the FCC's Technological Advisory Council Working Group on Artificial Intelligence and Computing at Appendix G, Section 13.5 (Jan. 14, 2021), https://www.fcc.gov/sites/default/files/fcc_aiwg_2020_whitepaper_final.pdf.

¹⁰² See O-RAN Alliance, *O-RAN Use Cases and Deployment Scenarios White Paper* at 5 (Feb. 2020) <https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/O-RAN+Use+Cases+and+Deployment+Scenarios+Whitepaper+February+2020.pdf>.

¹⁰³ See Fierce Wireless, *The Inherent Security of Open RAN* (Dec. 14, 2020), <https://www.fiercewireless.com/sponsored/inherent-security-open-ran>.

network operators have the resources to manage the deployment of Open RAN technology into their networks? Is this a task that smaller network operators can successfully manage? What institutional requirements and associated costs are required to support system integration? What role will system integrators perform in deployment of Open RAN technology?

2. Network Security and Public Safety

49. Could Open RAN architecture expose new security vulnerabilities that might not otherwise exist in a more closed architecture?¹⁰⁴ If open-source software fosters collaborative development among many stakeholders, does this enable a greater number of stakeholders to potentially discover vulnerabilities that might not otherwise be exposed and mitigated in closed systems? Or would the introduction of a greater number of stakeholders introduce vulnerabilities if appropriate care is not taken and software is not fully vetted by vendors or operators that choose to use open-software?¹⁰⁵ Does Open RAN introduce further issues raised by compromised trusted vendors, such as those that occurred during the SolarWinds breach?¹⁰⁶

50. Does Open RAN introduce any risks to the security and integrity of public safety communications? We seek comment on whether public facing infrastructures, like the RAN, are or may become an ideal target for bad actors to disrupt vital communications that rely on interoperability, such as 911, E-911, and NG 911 services (collectively referred to as 911). Similarly, is there a risk that prioritized public safety communications, such as those provided by FirstNet or the Wireless Priority Service, could also be subject to disruption from bad actors exploiting vulnerabilities in Open RAN that may not exist in a proprietary traditional RAN? Conversely, can Open RAN solutions remediate known vulnerabilities, such as False Base Stations, in proprietary RANs?¹⁰⁷ We seek comment on whether and, if so, how the use of Open RAN may introduce new and heightened security risks to the 911 system. Are these risks particularly heightened by the 911 system's interdependence with originating service providers, the continued operation of legacy public safety access points or emergency communications centers, and the ongoing migration of 911 services to NG 911? For example, it is commonly understood that security functions (like data encryption) to protect data traversing through the IP-based networks do not function or are unavailable as the data travel through legacy network elements.¹⁰⁸ Does the use of Open RAN exacerbate these concerns? Specifically, what other ways might the enhanced interconnectedness fostered by Open RAN increase the cyberthreat attack surface to 911 services? To what extent might Open RAN exacerbate the potential cyber threat from legacy public safety answering points that operate in hybrid environments? To the extent Open RAN introduces risks to public safety communications, what steps can be taken by stakeholders or the Commission to eliminate or mitigate these concerns? We also ask commenters to estimate the potential costs associated with the risk mitigation related to public safety arising from Open RAN development.

51. Do the attributes of Open RAN that support its versatility to identify, isolate, and remediate security risks or threats in the service architecture also highlight its potential security vulnerabilities? To what extent could use of Open RAN make the network more vulnerable to

¹⁰⁴ See Ericsson, *Security Considerations of Open RAN*, <https://www.ericsson.com/en/security/security-considerations-of-open-ran> (last visited Feb. 22, 2021).

¹⁰⁵ *Id.*

¹⁰⁶ See National Security Agency, *Detecting Abuse of Authentication Mechanisms* (Dec. 2020), https://media.defense.gov/2020/Dec/17/2002554125/-1/-1/0/AUTHENTICATION_MECHANISMS_CSA_U_OO_198854_20.PDF.

¹⁰⁷ See Association for Computing Machinery, *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks* (June 2019), <https://dl.acm.org/doi/10.1145/3307334.3326082>.

¹⁰⁸ See Communications Security, Reliability, and Interoperability Council VII, Report on the Current State of Interoperability in the Nation's 911 Systems at 5 (Mar. 2020), <https://www.fcc.gov/file/18394/download> (CSRIC VII, WG 4).

cyberthreats or unanticipated failures compared to a traditional mobile networking approach? Is there a risk that Open RAN vendors may not yet have the processes in place to address quickly and efficiently possible gaps or bugs that could otherwise be exploited by bad actors? Are accountability and trust reduced in environments with multiple vendors? What steps should we take to promote the diversity of vendors, while ensuring a high standard of security and trust similar to that provided by proprietary end-to-end solutions? Is there a heightened or new security risk introduced by relying on a few established and new suppliers with shorter track records? Technologies associated with Open RAN impact stakeholders across the supply chain, as well as in industries that rely on safe and reliable communications networks. What industry guidelines or standards are in place to ensure vendors remain accountable for their products and service? We seek comment on these issues.

52. Moreover, does the disaggregated nature of Open RAN emphasize the importance of adhering to 5G security specifications in both open and closed systems, since security considerations of these components already are defined in the 3GPP standards? Although use of open-source software may be a prominent feature of Open RAN, many 5G vendors and operators already rely on open-source software to accelerate delivery of digital innovation.¹⁰⁹ We seek comment on the effects of open-source software on network security from entities that have already deployed some variation of open-source software.

3. Open-Source Software Vulnerabilities

53. As noted earlier, the source code for open-source software is made available to the public, enabling anyone to copy, modify, or redistribute that code.¹¹⁰ Does this openness also introduce new risks to the network? Does the variety and diversity of open-source software options increase the possibility of incompatibilities in the system or make it more vulnerable to hacking or other vulnerabilities? To what extent are stakeholders applying inventory management of open-source components,¹¹¹ code management systems, testing of open-source code, and security frameworks to mitigate open-source risks as recommended by CSRIC?¹¹² We seek comment on whether the process for reviewing and accepting contributions to open-source software platforms may affect the security of Open RAN. For example, who verifies the integrity of those who seek to change the code? Are there existing criteria or processes used to select reviewers, and what processes are there to ensure that contributions made to change or edit the source code comport with existing security standards? For example, to what extent are Common Vulnerabilities and Exposures (CVEs) against open-source software components monitored? What safeguards and protocols are in place to thwart bad actors?¹¹³ To the extent that safeguards exist, are they implemented to meet the security standards expected by enterprises and service providers? Are there other risk factors we should be considering?¹¹⁴ An analysis of the benefits and challenges combined with ideas on how the Commission can support more secure, efficient, and resilient

¹⁰⁹ 5G Americas, *Security Considerations for the 5G Era White Paper* at 18 (July 2020), <https://www.5gamericas.org/wp-content/uploads/2020/07/Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf>.

¹¹⁰ See Communications Security, Reliability, and Interoperability Council VII, Report on Risk Introduced by 3GPP Release 15 and 16 5G Standards at § 5.11 (Sept. 2020), <https://www.fcc.gov/files/csric7reportriskintroducedby3gpppdf> (CSRIC VII, WG 3 Final Report).

¹¹¹ See National Telecommunications and Information Administration, Software Bill of Materials, <https://www.ntia.gov/SBOM> (last visited Feb. 22, 2021).

¹¹² See Communications Security, Reliability, and Interoperability Council, Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0 at 7-1 (Sept. 2018), <https://www.fcc.gov/file/14500/download>.

¹¹³ See Mitre, *Common Vulnerabilities and Exposures*, <https://cve.mitre.org/> (last accessed Feb. 16, 2021).

¹¹⁴ See The Linux Foundation, *Open Source Software Supply Chain Security*, Feb. 2020, https://www.linuxfoundation.org/wp-content/uploads/oss_supply_chain_security.pdf.

architectures should be provided while addressing this topic.

4. Risks of a Virtualized Operating Environment

54. Virtualization isolates applications from each other, thus minimizing or even eliminating their disruption on other applications running in other isolated containers.¹¹⁵ Is there a risk, however, that actors with unrestricted access to the operating system of the device, often referred to as root access, can bypass the intrinsic security virtualization and can access and/or alter any file, data, applications running on that hardware platform? We seek comment on the security vulnerabilities of the operating environment of virtualized software. Can vendors or providers protect against impermissible root access to the operating system if the hardware is produced by an untrusted source? What credentialing, safeguards or general operating standards exist to ensure that an actor with root access cannot abuse root access for malicious means. Another attack vector created by virtualization is side-channel attacks, where one container can learn information from an unrelated container.¹¹⁶ Are there mitigations to side-channel attacks? Are these mitigations in common use? If not, what is inhibiting their use? We ask commenters to estimate the costs associated with risk mitigation related to commercial applicants arising from Open RAN deployment.

55. *Artificial Intelligence and Machine Learning.* Some entities claim that using AI and ML in any product present the risk of false positives (i.e., an indication that a condition, such as a network intrusion or malware, exists when in fact it does not).¹¹⁷ Correcting false positives requires the input of time and human resources to investigate, and the remediation of a false problem or incorrectly configured optimization scheme might result in a service outage or other denial of service. Should AI/ML be leveraged to support and enhance the security features of an Open RAN deployment? If so, how?

5. Barriers to Adoption by Established Operators

56. Are the potential benefits of Open RAN, described above, available only in a greenfield deployment? Commenters should discuss the relative and absolute costs of incorporating Open RAN components into an established network. How can established RANs incorporate elements of Open RAN without replacing the entire network? Are there any obstacles that overlaying an Open RAN network on top of an existing early-generation closed network create? How scalable is the Open RAN concept to multi-gigabit wireless networks, such as non-standalone, millimeter-wave 5G cellular networks deployed in the U.S. that rely upon legacy, 4G LTE components? Do the potential cost reductions and performance enhancements due to disaggregation disappear once the costs of end-to-end multi-vendor interoperability testing are accounted for? Will this innovation and flexibility also maintain the stable operating environment that suppliers and consumers expect and demand of the nation's communications infrastructure?

6. Other Considerations

57. Are there any other factors to take into account when considering the viability and extent of open and virtualized RAN deployments? Will the fronthaul and midhaul between disaggregated units in the radio access network limit the deployment of Open RAN cell sites to areas where fiber or other high-capacity connections are available? Will the availability of fronthaul and midhaul options limit deployment of Open RAN networks to more densely populated areas? According to press reports, some

¹¹⁵ See Mavenir, *Understanding OpenRAN*, <https://mavenir.com/portfolio/access-edge-solutions/radio-access/understanding-openran-5g/> (last accessed Feb. 16, 2021).

¹¹⁶ See generally Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stegan Savage, *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*, Proceedings of the 16th ACM Conference on Computer and Communications Security, November 2009, pp. 199-212.

¹¹⁷ See generally Rafal Kocielnik, Saleema Amershi, Paul N. Bennett, *Will You Accept an Imperfect AI? Exploring Designs for Adjusting End-user Expectations of AI Systems*, (2019), https://www.microsoft.com/en-us/research/uploads/prod/2019/01/chi19_kocielnik_et_al.pdf.

original equipment manufacturers have expressed concerns regarding the energy efficiency of Open RAN equipment.¹¹⁸ Are these concerns valid? If so, then what steps could potentially be taken to reduce the energy consumption associated with this equipment? Are there other issues associated with deployment of open and/or virtualized RAN equipment that we should be aware of?

D. Potential Commission Efforts to Promote Development and Deployment

1. Identify Potential Barriers

58. Assuming we find that Open RAN could provide substantial public interest benefits, and subject to the cost-benefit considerations outlined below, we seek comment on whether we should enact rules, consistent with the Commission's rulemaking authority under current statutes, to promote reliability, interoperability, and adoption of Open RAN systems. Are Commission actions warranted to support the development of Open RAN standards? How can the Commission best harness industry experts to understand regulatory constraints impacting Open RAN deployments and the most appropriate regulatory approach moving forward? Commenters should identify aspects of the Open RAN system that require streamlined rules and a harmonized regulatory framework.

59. We seek comment on whether any of our existing rules impede Open RAN investment and development. Commenters should identify existing regulatory barriers hindering the continued development and proliferation of Open RAN solutions. We ask commenters to identify regulations that are outdated or unnecessarily burdensome to the development and deployment of Open RAN technologies, and whether the Commission should update, forbear from applying, or eliminate any of our existing rules in order to best serve the public interest. We also seek comment on whether there are any market inefficiencies that could be addressed by changes to the Commission's rules.

2. Testbeds and Demonstration Projects

60. In 2013, the Commission adopted rules creating the opportunity for expanded experimentation through Program experimental licenses and Innovation Zones.¹¹⁹ Under a Program experimental license, qualified institutions may conduct testing for multiple non-related experiments under a single authorization within a defined geographic area under control of the licensee and where the licensee has institutional processes to manage and oversee experiments. The Innovation Zone takes this concept a step further by effectively providing an extension of a Program License's authorized area of operation. Such licensees are permitted to operate within an Innovation Zone, under the parameters set for that particular Zone, without having to modify their licenses to cover the new location.¹²⁰ Innovation Zones can be created in response to a particular request or on the Commission's own motion.

61. The Commission has established two Innovation Zones – in New York City and Salt Lake City – to test new advanced technologies and prototype networks outside a traditional small campus

¹¹⁸ See Laurens Cerulus, Ericsson CEO: Don't waste time on Open RAN, Politico (Feb. 3, 2021), <https://subscriber.politicopro.com/tech/whiteboard/2021/02/ericsson-ceo-dont-wastetime-on-open-ran-3986785> (noting that, according to Ericsson, networks using O-RAN technologies could require up to 40 percent more energy to run); see also Jeanne Whalen, *A remote corner of Idaho has become the best hope for the U.S. challenge to Huawei*, Washington Post (June 29, 2020), <https://www.washingtonpost.com/business/2020/06/29/huawei-alternative-oran-idaho/> (“Even one of the new technology's biggest backers . . . says [Open RAN] manufacturers will have a hard time matching the energy efficiency of Huawei's radio heads unless the United States invests in better semiconductor technology.”).

¹¹⁹ *Promoting Expanded Opportunities for Radio Experimentation and Market Trials under Part 5 of the Commission's Rules and Streamlining Other Related Rules*, ET Docket No. 10-236, Report and Order, FCC 13-15, 28 FCC Rcd 758 (2013) (*Experimental R&O*).

¹²⁰ *Experimental R&O*, 28 FCC Rcd at 792, para 93.

or laboratory setting, including those that can support 5G technologies.¹²¹ These Innovation Zones permit experimentation across a wide variety of spectrum bands encompassing both non-federal and federal or shared allocations at power levels commensurate with commercial service. Could these Innovation Zones, either the two already created or new zones, provide opportunities to test and verify the security and operational benefits associated with Open RAN technology? Could Innovation Zones also be used to test and adjust various Open RAN parameters to optimize its implementation? We seek comment on these issues. Are there adjustments that we might need to make to these Innovation Zones to better enable Open RAN technology testing? Should other testbeds be established for this purpose? Should the Commission encourage or require the interconnection of testbeds to better simulate the challenges of actual network deployments? Are there other features of Open RAN technology that should be explored through such test beds or demonstration projects? For example, can such testbeds be used to evaluate system integration issues in mixed vendor environments both in terms of different Open RAN vendor equipment and a mix of Open RAN and more traditional network equipment operating in close proximity? Are there funding mechanisms in place for researchers to conduct the testing needed to advance Open RAN technology to a maturity level sufficient for widespread commercial deployment? How can the Commission incentivize stakeholder participation in test beds and/or demonstration projects? What features of such programs would attract stakeholder participation by increasing potential gains and reducing potential risks of participation? What other steps can the Commission take or programs can it put in place to encourage and enable development and testing of Open RAN technology?

62. Moreover, should the Commission have any role in promoting, developing or testing of Open RAN equipment? Are there any actions that the Commission should take to facilitate the integration and testing of Open RAN technology? How can the Commission encourage the development of Open RAN security and reliability? Could this involve the adoption of performance standards or other rules for Open RAN equipment? Should the Commission support research and development of technologies useful for Open RAN development? If so, how? If the Commission were to support Open RAN research and development activities, what types of technologies would be most useful to facilitate Open RAN adoption? Should the Commission sponsor Open RAN plugfests, either on its own or in partnership with other organizations, to encourage the development of interoperable Open RAN equipment and demonstrate its capabilities? What other actions can the Commission take to demonstrate and test the functionality of Open RAN network equipment? Finally, what timeframes are realistic for the completion of any study or analysis conducted as part of Open RAN network equipment being deployed in a testbed environment?

3. USF/Rip and Replace

63. The *Supply Chain Second R&O* created the Reimbursement Program, which will “reimburse the costs reasonably incurred by providers of advanced communications services . . . to permanently remove, replace, and dispose of covered communications equipment and services from their networks.”¹²² In adopting the Reimbursement Program, the Commission recognized that “a certain level of technological upgrade is inevitable . . .” when replacing older technology. Thus, the Commission’s Reimbursement Program permits “participants to obtain reimbursement for reasonable costs incurred for

¹²¹ *Office of Engineering and Technology Announces First Innovation Zones for Program Experimental Licenses*, ET Docket No. 19-257, Public Notice, DA 19-923, 34 FCC Rcd 8130 (OET 2019).

¹²² *Supply Chain Second R&O*, 35 FCC Rcd at 14331, para. 108. Section 3 of the Secure Networks Act bans the use of “a federal subsidy that is made available through a program administered by the Commission and that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service” to purchase, rent, or otherwise obtain any covered communications equipment or services published on the Commission’s Covered List. Secure Networks Act § 3(a). In the *2019 Supply Chain Order*, the Commission adopted a similar prohibition on the use of USF funds to “purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain.” *2019 Supply Chain Order*, 34 FCC Rcd at 11488, Appendix A; 47 CFR § 54.9.

replacing older mobile wireless networks with fourth generation Long Term Evolution (4G LTE) equipment or services that are 5G ready.”¹²³ While the Commission expected providers to “obtain the lowest-cost equipment that most closely replaces their existing equipment . . . ,” it recognized that “replacement of older legacy technology will inevitably require the use of newer equipment and services that have additional capabilities.”¹²⁴ This position is consistent with both Congressional intent, which “expects there to be a transition from 3G to 4G or even 5G-ready equipment in instances where equipment being replaced was initially deployed several years ago,”¹²⁵ and with market developments which indicate “new equipment supporting older, second- and third generation wireless technology services is unavailable, and even acquiring such equipment and services on the secondary market is proving increasingly difficult and in some instances impossible.”¹²⁶ Thus, providers may have an opportunity to replace the unsecure equipment and services, consistent with the *Supply Chain Second R&O*, with Open RAN equipment and services that could work in a multi-vendor network and architecture. Given the potential advantages of Open RAN technology and virtualized components in a multi-vendor network solution, we seek comment on whether we should take additional steps to support this deployment.

64. Section 4(d)(1) of the Secure Networks Act directs the Commission to create a list of suggested replacements (Replacement List) for the equipment and services being removed, replaced, and destroyed.¹²⁷ The Replacement List must include “both physical and virtual communications equipment, applications and management software, and services or categories of replacements of both physical and virtual communications equipment, application and management software and services.”¹²⁸ Importantly, this list must be “technology neutral.”¹²⁹ In the Secure Networks Act, Congress explicitly supported the potential inclusion of services such as Open RAN and virtualized network equipment on the Replacement List “to the extent that the Commission determines that communications services can serve as an adequate substitute for the installation of communications equipment.”¹³⁰ The Commission made such a finding in the *Supply Chain Second R&O*.¹³¹ Thus, Open RAN and other services are eligible to be included on the Replacement List and the Commission encouraged “providers participating in the Reimbursement Program to consider this promising technology” along with other technologies as they made their procurement decisions.¹³²

65. While the Replacement List is only a “suggested” list for the types of equipment and services providers may use to secure their networks, we believe including Open RAN and other virtualized equipment and services will help promote Open RAN development and deployment. Are there additional actions the Commission could take to encourage deployment and development of Open RAN through the Replacement List? If so, what precise actions should the Commission take? What would be the likely outcome? How can the Commission support and encourage the deployment and development of Open RAN through the Replacement List while also complying with the obligation in the Secure Networks Act that the Replacement List be technology neutral? Specifically, we seek comment on whether it is possible to comply with the requirement that the Replacement List be technologically

¹²³ *Supply Chain Second R&O*, 35 FCC Rcd. at 14336, para. 122.

¹²⁴ *Id.*, 35 FCC Rcd at 14337, para. 125.

¹²⁵ H.R. Rep. No. 116-352, at 13.

¹²⁶ *Supply Chain Second R&O*, 35 FCC Rcd at 14338, para. 126 (footnote omitted).

¹²⁷ 47 U.S.C. § 1603(d)(1)(A).

¹²⁸ *Id.*

¹²⁹ *Id.* § 1603(d)(1)(b).

¹³⁰ *Id.*

¹³¹ *Supply Chain Second R&O*, 35 FCC Rcd at 14366, para. 202.

¹³² *Id.*

neutral, while also supporting the growth and development of new technologies. In the event the Commission took additional steps to encourage the deployment and development of Open RAN through the Replacement List, what are the potential impacts to the Reimbursement Program? How would these steps impact the deployment and development of Open RAN?

66. The *Supply Chain Second R&O* allowed providers of advanced communications service to begin removing insecure equipment now while being reimbursed once the Reimbursement Program is ready to accept applications.¹³³ We seek comment on whether providers of advanced communications services, especially small providers, are adopting Open RAN or virtualized solutions as they replace covered equipment in their networks. We also seek comment on whether providers that have not begun the remove and replace process are considering Open RAN. Alternatively, are providers considering or deploying equipment that could support or be upgraded to support Open RAN or virtualized equipment in the future? We seek comment on what steps the Commission could take to encourage providers to deploy Open RAN technology. If providers are not considering Open RAN, or are hesitant to deploy Open RAN and virtualized technology, we seek comment on why and on what steps the Commission could and should take to encourage providers of advanced communications service, especially small providers, to consider or select Open RAN as part of the technological offerings available for replacement going forward. The Secure Networks Act imposes short deadlines to make certain the remove and replace process is completed expeditiously.¹³⁴ However, the Secure Networks Act also allows for an individual extension of a provider's deadline in limited circumstances.¹³⁵ Could the Commission grant an extension for providers seeking to deploy Open RAN or virtualized network equipment and services? Would such an extension incentivize providers to deploy Open RAN? We seek comment on whether granting extensions in this manner would be consistent with the Secure Networks Act.

67. We also seek comment on whether the Reimbursement Program affords us any other opportunities to encourage the deployment or development of Open RAN technology beyond the Replacement List. The Secure Networks Act does not expressly prohibit the Commission from encouraging providers who choose to replace the covered equipment and services in their networks with any particular type of replacement equipment. The technological neutrality obligation is expressly limited to the items included in the Replacement List.¹³⁶ Can the Commission offer any additional incentives to Reimbursement Program participants who choose to replace their covered equipment or services with Open RAN technology? If so, what types of incentives would most benefit such providers? Is the Open RAN technology sufficiently developed where providers of advanced communications services can purchase this equipment or services on the open market? Does the cost to providers make this equipment or these services competitive with other types of equipment or services? We expect providers would be faced with increased upfront costs for this equipment. Would any increased upfront purchase costs be offset by reduced costs elsewhere, such as reduced maintenance costs needed to support a virtualized network? Are there other costs that could be covered by the Reimbursement Program? Can the Reimbursement Program cover the expenses for system integrators to configure the network infrastructure for many carriers? What other expenses will providers deploying Open RAN encounter? We also seek comment on whether this technology simply would replace the insecure equipment and services being removed from communications networks, or does it require different infrastructure that would further burden providers or the Reimbursement Program?

68. Finally, we seek comment on whether other Universal Service Fund support can be used to incentivize the development and deployment of Open RAN or virtualized systems. One of the Commission's central missions is to make "available . . . to all the people of the United States . . . a rapid,

¹³³ *Id.*, 35 FCC Rcd at 14340, para. 130.

¹³⁴ Secure Networks Act § 4(d)(6)(B).

¹³⁵ *Id.* § 4(d)(6)(C).

¹³⁶ *Id.* § 4(d)(1)(b).

efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges.”¹³⁷ As the Commission has observed, with the passage of the Telecommunications Act of 1996, Congress “directed the Commission and states to take steps necessary to establish support mechanisms to ensure delivery of affordable telecommunications services to all Americans, including low-income consumers, eligible schools and libraries, and rural health care providers.”¹³⁸ Specifically, Congress set forth certain specific principles for universal service advancement.¹³⁹ The Commission has followed these principles in establishing and occasionally reforming its Universal Service policies, including efforts to “ensure[] that all consumers . . . benefit from the historic transitions that are transforming our nation’s communications services.”¹⁴⁰ How would supporting Open RAN further the section 254(b) principles, upon which the Commission must base its universal service policies?

4. Operational/Service Rules

69. We note that the Commission has traditionally adopted a policy of technology neutrality and we seek comment on whether changes are necessary to ensure our rules remain technologically and competitively neutral as Open RAN technologies are integrated into wireless networks. Commenters should identify whether any of our existing rules unfairly advantage or disadvantage one RAN technology over another. For example, do our rules favor or disadvantage either a single vendor or multi-vendor approach? We ask commenters to identify these rules and suggest changes that would address these concerns. What changes are necessary to ensure our rules remain technologically neutral?

70. A Commission licensee is responsible for ensuring that its network complies with the Communications Act and Commission rules. Would a licensee that chooses to incorporate into its network an Open RAN technology that is comprised of multiple components supplied by multiple vendors face different challenges than a licensee that has multiple vendors for non-RAN components or different RAN vendors today? We seek comment on ways to ensure that licensees maintain responsibility for each element of their network in accordance with the Communications Act and Commission rules. Does Open RAN present unique challenges in this regard? If so, how should we account for those challenges in the service rules for each band? We also seek comment on how testing of Open RAN equipment for compliance with the Commission’s technical rules could be accomplished as part of the equipment certification process? Commenters should identify other challenges that entities deploying Open RAN technologies may face in complying with existing operational and service rules.

5. Commission Outreach and Information Gathering

71. As discussed, the Commission has previously promoted industry and public involvement in Open RAN discussions. The Commission’s Technological Advisory Committee provides technical advice to the Commission, and one of its four working groups recently studied virtualized radio access

¹³⁷ 47 U.S.C. § 151.

¹³⁸ *Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, Report and Order, 12 FCC Rcd 8776, 8780, para. 1 (1997).

¹³⁹ 47 U.S.C. § 254(b). First, quality service should be available at just, reasonable, and affordable rates. *Id.* § 254(b)(1). Second, access to advanced telecommunications and information services should be provided nationwide. *Id.* § 254(b)(2). Third, consumers nationwide, including in rural and high cost areas, should have access to services that are reasonably comparable to services in urban areas and at similar rates. *Id.* § 254(b)(3). Fourth, all providers of telecommunications services should make an equitable and nondiscriminatory contribution for universal service. *Id.* § 254(b)(4). Fifth, there should be specific, predictable, and sufficient federal and state mechanisms to preserve and advance universal service. *Id.* § 254(b)(5). And, sixth, schools, health care providers, and libraries should have access to advanced telecommunications services. *Id.* § 254(b)(6). The Commission may also adopt additional principles. *Id.* § 254(b)(7); *see, e.g., Connect America Fund*, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 17679, paras. 44-45 (2011) (adopting a principle that universal service support “should be directed where possible to networks that provide advanced services, as well as voice services”).

¹⁴⁰ *Connect America Fund, et al.*, WC Docket No. 10-90, et al., Report and Order, 29 FCC Rcd 15644, para 2 (2014).

networks as well as 5G technology and the Internet of Things applications. We seek comment on the recommendations of this working group.¹⁴¹ We seek further comment on how best to harness the work of the TAC or other potential groups that the Commission could establish, in order to engage government, industry, and academia stakeholders in developing and deploying Open RAN solutions.

72. As discussed above, CSRIC has previously examined security issues in 5G networks. To what extent should potential future iterations of CSRIC¹⁴² be used to promote Open RAN technology without endorsing a particular technology or company? What other roles might CSRIC serve to foster Open RAN development and security?

73. *Relationship to Other Federal Agencies.* The National Science Foundation has funded fundamental research on open architectures for many years. The most recent program, Platforms for Advanced Wireless Research (PAWR), is a public-private partnership that seeks to develop experimental testbeds for innovative research into the next generation of wireless systems.¹⁴³ One such testbed is the Platform for Open Wireless Data-driven Experimental Research (POWDER), a facility for Open RAN experimentation, by both academia and industry, in a city-scale “living laboratory” run by the University of Utah in partnership with Salt Lake City and the Utah Education and Telehealth Network.¹⁴⁴ POWDER will deploy and test both off-the-shelf equipment and radio hardware and software being developed by RENEW (Reconfigurable Eco-system for Next Generation End-to-end Wireless), a partnership of Rice University, University of Michigan, and Texas Southern University focused on developing a fully programmable and observable wireless radio network.¹⁴⁵ Likewise, the Cloud Enhanced Open Software-Defined Mobile Wireless Testbed in New York City provides city-scale wireless experimentation for ultra-high bandwidth and low latency technologies and applications.¹⁴⁶

74. DARPA recently started the Open, Programmable, Secure 5G (OPS-5G) program to address security challenges that will confront future wireless networks.¹⁴⁷ OPS-5G aims to reduce reliance on potentially untrusted providers of technology by developing a secure-by-design stack for mobile, wireless networks using open-source software and interoperable, standard-compliant hardware and software components. NTIA recently announced a 5G Challenge Notice of Inquiry¹⁴⁸ in collaboration with the Department of Defense (DoD) 5G initiative, seeking feedback on the creation of a 5G Challenge that will spur stakeholders into accelerating deployment of Open RAN architectures in the recently announced DoD 5G test-beds. The Notice of Inquiry is structured around three main categories of questions: (i) challenge structure and goals, (ii) incentives and scope, and (iii) timeframe and infrastructure support.

¹⁴¹ Federal Communications Commission, *Technological Advisory Council (TAC) Meeting* at 14 (December 1, 2020), <https://www.fcc.gov/sites/default/files/tac-presentations-12-1-20.pdf>.

¹⁴² The current CSRIC term ends on March 14, 2021. The Commission has not announced whether CSRIC will be renewed for a new term.

¹⁴³ Platforms for Advanced Wireless Research, *About PAWR*, <https://advancedwireless.org/about-pawr/> (last visited Feb. 22, 2021).

¹⁴⁴ Platform for Open Wireless Data-driven Experimental Research, *Powder-RENEW*, <https://powderwireless.net/> (last visited Feb. 22, 2021).

¹⁴⁵ *Id.*, see also RENEW, *World’s First Fully Programmable and Open-source Massive-MIMO Platform*, <https://renew.rice.edu/> (last visited Feb. 22, 2021).

¹⁴⁶ See PAWR, *Advanced Wireless, New York City*, <https://advancedwireless.org/new-york-city/> (last visited Feb. 22, 2021).

¹⁴⁷ See Defense Advanced Research Project Agency, *Open, Programmable, Secure 5G (OPS-5G)*, <https://www.darpa.mil/program/open-programmable-secure-5g> (last visited Feb. 22, 2021).

¹⁴⁸ NTIA, *5G Challenge Notice of Inquiry*, Docket No. 210105-0001, Notice of Inquiry, 86 Fed. Reg. 1949 (Jan. 11, 2021) (*NTIA 5G Challenge NOI*). Comments were due on Feb. 10, 2021.

75. The DoD has awarded \$600M in the first phase of funding (called Tranche 1) to 15 prime contractors to evaluate 5G technologies in five military installations across the United States.¹⁴⁹ Each will investigate a specific application such as AR/VR based training, “smart warehousing” capability, and spectrum sharing between radar and cellular services. In addition, seven sites have been chosen for Tranche 2.¹⁵⁰ The solicitation period for white papers for four of the sites in Tranche 2 closed on December 15, 2020, and the process of evaluating these has begun. Request For Proposals for all seven sites in Tranche 2 are expected in early 2021.¹⁵¹

76. Is there a role for the FCC in helping to advance the objectives of these various federal efforts to promote and streamline Open RAN development and deployment? How can the Commission ensure that it is not duplicating efforts of other federal agencies or contribute to these ongoing initiatives? Should the FCC help to facilitate industry engagement in these processes to ensure that the interests of non-federal operators and equipment manufacturers are adequately represented?

77. *Role in International Open RAN Efforts.* The Commission’s regulatory counterparts around the world are exploring Open RAN within the context of their respective domestic regulatory policy. The United Kingdom, for example, is creating a SmartRAN Open Network Interoperability Centre as a part of its national 5G Diversification Strategy.¹⁵² The center is a joint program between the UK regulator Ofcom and UK innovation agency Digital Catapult, and it will serve as a testbed for Open RAN solutions.¹⁵³ Likewise, in Japan, the Ministry of Internal Affairs and Communications has outlined plans to pursue international collaboration in order to promote the implementation and standardization of open architecture and network virtualization.¹⁵⁴ Germany has begun to consider providing funding for Open RAN research and development, as the United States has done.¹⁵⁵

78. International fora have also increasingly begun to engage in dialogue on Open RAN. For instance, in February 2021, the United States co-sponsored a workshop on open architectures and network virtualization within the Telecommunications & Information Working Group of the Asia-Pacific

¹⁴⁹ Department of Defense, *DOD’s Inaugural Foray Into 5G Experimentation on Track* (Jan. 5, 2021), <https://www.defense.gov/Explore/News/Article/Article/2462765/dods-inaugural-foray-into-5g-experimentation-on-track/>.

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² UK Department for Digital, Culture, Media and Sport, *5G Supply Chain Diversification Strategy* (Dec. 7, 2020), <https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy>.

¹⁵³ Digital Catapult, *DCMS 5G Diversification Strategy Leads to UK Interoperability Push* (Nov. 29, 2020), <https://www.digicatapult.org.uk/news-and-insights/press/dcms-5g-diversification-strategy-uk-interoperability-push-digital-catapult>; Ofcom, *Supporting the U.K.’s Wireless Future: Our Spectrum Management Strategy for the 2020s* (Dec. 4, 2020), https://www.ofcom.org.uk/data/assets/pdf_file/0027/208773/spectrum-strategy-consultation.pdf.

¹⁵⁴ Ministry of Internal Affairs & Communications (MIC), *Beyond 5G Promotion Strategy (Overview)* (June 2020), https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/200414_B5G_ENG_v01.pdf. In response to the full-scale software development and virtualization of communications networks, MIC has also explored partial revision of its Standards for Safety and Reliability of Information and Telecommunications Networks. MIC, *Results of Appeal for Opinions on Draft Notice for Partial Revision of Standards for Safety and Reliability of Information and Telecommunications Networks* (May 25, 2020), https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/5/25_1.html.

¹⁵⁵ Politico, *Berlin’s €2B plan to wean off Huawei (Nokia and Ericsson too)* (Feb. 2, 2021), <https://www.politico.eu/article/germany-huawei-telecoms-plan/>.

Economic Cooperation forum (APEC).¹⁵⁶ The European Commission has also launched a study into the status of 5G supply markets and Open RAN and has held workshops with stakeholders to gather information.¹⁵⁷

79. These initiatives lead us to ask broadly whether the experiences of other telecommunications regulators provide any best practices or lessons learned that the Commission should consider, especially keeping in mind the international nature of current and planned Open RAN deployments. Are there lessons we should learn from our counterparts abroad about how an independent regulator can best support national research and development efforts? With which specific organizations or events should the Commission consider participating in order to have productive international discussions on Open RAN? As one of many U.S. agencies working alongside the Department of State to engage with organizations like APEC and the OECD, what specific role can the Commission play to ensure any OECD principles or best practices identified by those organizations serve the public interest? Is there information that we should be gathering from, or sharing with, international stakeholders on Open RAN, and, if so, what is the most appropriate avenue by which we should gather or share this information? Finally, are there any steps the Commission can or should take to support industry-led efforts internationally and help avoid fragmentation or duplication? How can the Commission encourage U.S. stakeholders to participate in these fora?

6. Legal Issues

80. The Commission has broad authority under Title III of the Act to manage the use of radio spectrum, to prescribe the nature of wireless services to be rendered, and to modify existing licenses when doing so would promote the public interest.¹⁵⁸ We seek comment on what additional legal obligations may incentivize and support the development and deployment of more secure Open RAN. For example, in adopting the Commission's prohibition on the use of USF funds to purchase, operate, or maintain covered communications equipment and services, the Commission found that the rule implicated section 105 of CALEA.¹⁵⁹ Section 105 requires every telecommunications provider to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer of employee of the carrier."¹⁶⁰ The Commission found that, therefore, telecommunications carriers¹⁶¹ "appear to have a duty" to avoid the risk that an untrusted

¹⁵⁶ APEC Project Database, *Report and Workshop on Network Virtualization, Disaggregated Networks and Open Telecommunication Architecture in APEC*, <https://aimp2.apec.org/sites/PDB/Lists/Proposals/DispForm.aspx?ID=2609> (last visited Feb. 11, 2021).

¹⁵⁷ European Commission, *European Commission Launches Study into 5G Supply Markets and Open RAN* (July 24, 2020), <https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-study-5g-supply-markets-and-open-ran>; European Commission, *Stakeholder Workshop on 5G Supply Market Trends, and Perspectives on Open Initiatives* (Dec. 3, 2020), <https://ec.europa.eu/digital-single-market/en/news/stakeholder-workshop-5g-supply-market-trends-and-perspectives-open-initiatives>.

¹⁵⁸ See, e.g., 47 U.S.C. §§ 301, 302, 303, 309.

¹⁵⁹ *2019 Supply Chain Order*, 34 FCC Rcd at 11436, para. 35. CALEA is the Communications Assistance for Law Enforcement Act, Pub. L. 103-414, 108 Stat. 4279 (1994) (CALEA) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.).

¹⁶⁰ 47 U.S.C. § 1004.

¹⁶¹ The definition of "telecommunications carrier" that applies in CALEA is broader than, but inclusive of, the definition in the Communications Act. Compare 47 U.S.C. § 1001(8) with § 153(51); see *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989, 14992-97, paras. 9-14 (2005) (*2005 CALEA Order*), *pet. for rev. denied*, *American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006). The Commission has concluded that all facilities-based providers of broadband Internet access services and all providers of interconnected VoIP services are telecommunications carriers under CALEA. *2005 CALEA Order*, 20 FCC Rcd at 14989, para. 1.

supplier could illegally intercept or provide remote unauthorized network access by the insertion of malicious hardware or software implants.¹⁶² We seek comment on the impact of virtualized and interoperable network components on a carrier's ability to comply with this statutory obligation. Would disaggregation of the RAN functionality and an enhanced ability to use network elements from different vendors help network operators ensure that carriers can prevent access to their networks by untrusted entities?

81. In addition to the statutory obligation, the Commission is authorized to “prescribe such rules as are necessary to implement the requirements of” CALEA and to require carriers to establish policies to prevent unauthorized surveillance.¹⁶³ When adopting section 54.9, the Commission found that that rule directly implements section 105 of CALEA by reducing the likelihood that ETCs use USF support to facilitate unauthorized surveillance.¹⁶⁴ Can the Commission rely upon CALEA obligations and its associated rulemaking authority to encourage deployment of secure equipment, including Open RAN? We also seek comment on whether CALEA provides authority to support the development and deployment of Open RAN. For example, section 106 directs manufacturers to make available to carriers, “on a reasonable and timely basis and at a reasonable charge, ... such features or modifications as are necessary to permit such carriers to comply with the capability requirements” of section 103;¹⁶⁵ those capability requirements include the ability to facilitate authorized surveillance “in a manner that protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted” and “information regarding the government’s interception of communications and access to call-identifying information.”¹⁶⁶

82. Congress has directed the Commission to “encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans ... by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment.”¹⁶⁷ What sources of authority could the Commission consider invoking to encourage or incentivize development and deployment of Open RAN and virtualized networks? In the *Supply Chain Second Report and Order*, the Commission relied upon sections 201(b) and 254, among other sections, for authority to require USF recipients to remove and replace covered equipment.¹⁶⁸ Do those sections provide the Commission with authority to encourage and incentivize development and deployment of Open RAN and virtualized networks? If so, should the Commission rely upon these sections to do so? Commenters should explain in detail why or why not they believe we have authority to act, if the Commission chooses to do so.

E. Costs and Benefits of Open RAN Deployment

83. We seek comment on the likely costs and benefits of Open RAN deployment for mobile network operators. The Office of Economics and Analytics plans to undertake an economic study that would evaluate the likely benefits and costs of Open RAN deployment. In particular, we ask that commenters provide information and data that quantify both the potential costs and benefits of Open

¹⁶² 2019 *Supply Chain Order*, 34 FCC Rcd at 11436, para. 35.

¹⁶³ 47 U.S.C. § 229(a), (b)(1).

¹⁶⁴ 2019 *Supply Chain Order*, 34 FCC Rcd at 11437, para. 36. When the Commission adopted the remove and replace requirement for Eligible Telecommunications Carriers that receive Universal Service support, it found sufficient authority under sections 201(b) and 254 to act, and did not consider whether CALEA provided a legal basis for regulation. *Supply Chain Second R&O*, 35 FCC Rcd at 14297, para. 27 n.75.

¹⁶⁵ 47 U.S.C. § 1005.

¹⁶⁶ 47 U.S.C. § 1002(a)(4)(A), (B).

¹⁶⁷ 47 U.S.C. § 1302(a).

¹⁶⁸ *Supply Chain Second R&O*, 35 FCC Rcd at 14291, 14373, paras. 19, 225.

RAN deployment, and we seek comment on the issues that should be studied and likely promising methodologies to carry out such studies. For example, to what extent will mobile network operators benefit from open interfaces and standards? How would the Commission's actions impact the development of Open RAN and related technologies in comparison to what industry participants currently expect? Specifically, are there any obstacles preventing the industry from optimally investing in the Open RAN technologies that could be eliminated by Commission actions? Are there any spillover social benefits arising from the Open RAN deployment not internalized by the wireless network industry in its investment decisions? For example, does one firm's investment in the Open RAN system result in any spillover benefits to other Open RAN component vendors network operators, consumers, or public safety without such benefiting entities paying for the cost of development either directly or indirectly? We ask commenters to quantify the potential spillover social benefits that may be lost if the Open RAN development and deployment decisions are made by the wireless network firms, without Commission action.

84. We seek comment on the relative and absolute costs of Open RAN deployment and interoperability. How do the costs of Open RAN equipment compare with the costs of equipment from proprietary equipment manufacturers? How do the operating expenses of an Open RAN network compare to those of a proprietary network. Are there any costs to using multiple equipment vendors in constructing networks, such as the costs of network design and integration? If so, we ask commenters to provide information on the magnitude of these costs, and the underlying methodology for quantifying these costs. We also seek information on how interoperability between the various equipment vendors can be ensured. In particular, does it require specific integration platforms or institutions to monitor and coordinate the development and maintenance of standards and integration of the Open RAN technologies? If such institutions exist, are there Commission rules that would affect their operations? If such institutions do not exist, what are the associated costs to set up and maintain such platforms and institutions. Further, we seek information on Open RAN performance compared to existing networks or potential alternative technologies, and how the cost of deployment and relative benefits of performance differ. Do such differences depend on market characteristics such as whether areas are sparsely or densely populated or whether expanding geographic coverage or expanding capacity in a fixed geography is the more important consideration? To the extent that performance differs, we ask commenters to quantify the effect of those performance differences on consumers.

85. In addition, we seek comment on the likely costs and benefits of Open RAN for the broader economy. Could adopting Open RAN reduce the probability of security breaches compared with existing and alternative technologies? What are the economic costs of these breaches, including costs associated with breach prevention, that may vary across Open RAN and other technologies? How much additional consumer value and utilization of services would there be once networks implement Open RAN? How much would consumers value reduction in security risk from Open RAN deployment? How much would consumers value improvement in speed, additional capacity, or improvements in use cases such as drone operation? We seek comment on the costs of addressing security concerns raised elsewhere in this document.

IV. PROCEDURAL MATTERS

86. *Ex Parte Rules.* This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.¹⁶⁹ Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation

¹⁶⁹ 47 CFR § 1.1200(a). Although the Rules do not generally require *ex parte* presentations to be treated as "permit but disclose" in Notice of Inquiry proceedings, *see* 47 CFR § 1.1204(b)(1), we exercise our discretion in this instance, and find that the public interest is served by making *ex parte* presentations available to the public, in order to encourage a robust record. *See id.* § 1.1200(a).

must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Rule 1.1206(b), 47 CFR § 1.1206(b). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

87. *Comment Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS) or by paper. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

- Electronic Filers: Comments may be filed electronically by accessing ECFS at <https://www.fcc.gov/ecfs>.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. Paper filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail.
 - Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19.¹⁷⁰
 - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
 - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington, D.C. 20554.

88. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. These documents will also be available for public inspection during regular business hours in the FCC Reference Information Center, when FCC Headquarters reopens to the public.

89. *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

90. *Further Information.* For additional information on this proceeding, contact Jaclyn Rosen of the Mobility Division, Wireless Telecommunication Bureau, at jaclyn.rosen@fcc.gov or (202) 418-0154 or Mary Claire York of the Mobility Division, Wireless Telecommunications Bureau, at maryclaire.york@fcc.gov or (202) 418-2205.

V. ORDERING CLAUSES

91. Accordingly, IT IS ORDERED, pursuant to Sections 1, 303(g), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 303(g), and 403, and Section 1.430 of the Commission's rules, 47 CFR § 1.430, that this NOTICE OF INQUIRY IS ADOPTED.

¹⁷⁰ See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, 35 FCC Rcd 2788 (2020), <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary