ENERGY & COMMERCE
CHAIR RODGERS

MEMORANDUM

To: Members, Energy and Commerce Committee
From: Majority Staff
Re: Communications and Technology Subcommittee Hearing

I. INTRODUCTION

On Wednesday, January 17, 2024, at 10:00 a.m. (ET), the Subcommittee on Communications and Technology will hold a hearing in 2123 Rayburn House Office Building titled "Strengthening American Communications Leadership with Open Radio Access Networks."

II. WITNESSES

- John Baker, Senior Vice President of Ecosystem Business Development, Mavenir
- Jeff Blum, Executive Vice President, External & Government Affairs, DISH
- Diane Rinaldo, Executive Director, Open RAN Policy Coalition
- Kristian Toivo, Executive Director, Telecom Infra Project

III. BACKGROUND

Fifth-generation (5G) wireless technology is now being deployed across the world and touches nearly every sector of the economy. The growth of high-capacity, low latency mobile broadband allows the creation of digital applications that drive innovation. This leads to factory and farm automation, autonomous vehicles, and a network of connected devices that gather and leverage enormous amounts of data to increase the efficiency of most machines and appliances. As communications providers continue to deploy 5G, efforts are already underway to develop 6G, the next generation of wireless technology.

As wireless technologies evolve, some mobile network operators have explored technical changes to the network component known as the Radio Access Network (RAN). At its core, a RAN connects devices to the core network through a radio link.[1]

Today's RAN technology operates using an integrated package of hardware and software, many times locking carriers into a single supplier's proprietary system that is largely not interoperable with hardware or software developed by another supplier.[2] Because of the high barriers to enter the marketplace, and the need to invest billions of dollars annually in research

---

[1] *See* Dan Jones & Corinne Bernstein, What is radio access network?, TechTarget (Apr. 2021), https://www.techtarget.com/searchnetworking/definition/radio-access-network-RAN.
[2] *See* Melissa K. Griffith, Open RAN and 5G: Looking Beyond the National Security Hype, The Wilson Center (Nov. 2, 2020), https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype.

and development to stay competitive, the RAN marketplace has consolidated over time.[3] This has left mobile network operators fewer choices for trusted network equipment. As a result, some operators turn to untrusted vendors due to their ability to offer equipment at lower costs, which can be state-supported entities that are controlled by adversaries and threaten U.S. network security.

Two developments—Virtualized Radio Access Networks (V-RAN) and Open Radio Access Networks (O-RAN)—present opportunities to change this reality. Technical experts believe networks that integrate V-RAN and O-RAN architectures could improve the security of networks.[4] (Radio access networks can be "virtualized" without being "open.") Others have argued that deploying mobile networks with O-RAN could promote competition in the vendor marketplace, diversify the supply of trusted vendors, and decrease prices.[5] The development of open and virtualized network technology by mobile network operators and vendors is poised to bolster U.S. wireless leadership, U.S. companies, and could improve the security of U.S. mobile networks.

Virtualized Radio Access Networks (V-RAN)

V-RAN decouple purpose-built software and hardware so that software can be used on commercial-off-the-shelf equipment. This means mobile network operators can purchase cheaper, "dumb," antennas that can be programmed by sophisticated software solutions, lowering costs and providing greater flexibility. By virtualizing components of the RAN, mobile network operators can make changes to a RAN's software components through the cloud.

Open Radio Access Networks (O-RAN)

O-RAN would standardize the technologies within a RAN and require that various components within the network be interoperable regardless of manufacturer or vendor. Today, without O-RAN architecture, the proprietary interfaces among various components of the RAN are not interoperable because they are produced by a single vendor end-to-end . Economies of scale are significant in this legacy RAN system, since a firm needs far more resources to produce a full technology stack than to focus on only one or a few components in the open system. As a result, these technologies can be more expensive and the number of firms able to compete in the market is limited.

Deploying O-RAN technology could allow the many components of a RAN to operate with one-another regardless of which company produced each component by standardizing the interfaces that permits interoperability. As a result of this interoperability, many see this as one

---

[3] See, Nalma Hoque Essing, Jeff Loucks, et al., *The next-generation radio access network: Open and virtualized RANs are the future of mobile networks,* DELOITTE INSIGHTS (Dec. 7, 2020), https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/radio-access-networks.html/#endnote-15.

[4] *See*, 451 Research, *Security Benefits of Open Virtualized RAN,* S&P GLOBAL MARKET INTELLIGENCE (May 2020), https://www.redhat.com/cms/managed-files/ve-451-research-telco-vran-security-analyst-material-f23695-en.pdf.

[5] *See*, Robert D. Atkinson, Doug Brake, and Alexandra Bruer, *Open Radio Access Networks: A Primer for Policymakers,* INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (Nov. 1, 2021), https://itif.org/publications/2021/11/01/open-radio-access-networks-primer-policymakers/.

path for increasing market competition by lowering barriers to entry for any single component in the RAN. Mobile network operators and equipment vendors have been collaborating on technical standards to facilitate the deployment of virtualized and open networks for several years.[6]

IV. SELECT ISSUES

1. Public Wireless Supply Chain Innovation Fund

The Public Wireless Supply Chain Innovation Fund (Innovation Fund), authorized under the FY 2021 National Defense Authorization Act[7] and funded through the CHIPS and Science Act of 2022,[8] was enacted to support research and development of O-RAN in the United States. One goal was to support the growth of domestic equipment manufacturers--the largest equipment manufacturer globally is Chinese-based Huawei, while the next two are also based outside the United States—Ericsson (Sweden) and Nokia (Finland).[9] The Innovation Fund provides grants to facilitate the promotion and deployment of O-RAN networks by accelerating commercial deployment of interoperable 5G equipment; promoting a multi-vendor environment; identifying compliance standards; and promoting security features in these networks.[10]

Since releasing the initial Notice of Funding Opportunity on April 12, 2023,[11] the National Telecommunications and Information Administration (NTIA) has awarded over $98 million.[12] These awards fund research in energy-efficiency, improving O-RAN testing with data-driven and generative artificial intelligence (AI) testing methods, and the continued development of research in secure and adaptive spectrum sharing.

2. Deployment of O-RAN Networks

Although research and development of O-RAN continues, providers have already deployed O-RAN networks in the U.S. and around the world. DISH Wireless built the nation's first virtualized O-RAN 5G network.[13] AT&T plans to start deploying O-RAN sites this year in partnership with Ericsson,[14] while Verizon has deployed 8,000 V-RAN sites across the

---

[6] *See*, *O-RAN Specification,* O-RAN ALLIANCE (accessed Jan. 11, 2024), https://www.o-ran.org/specifications.
[7] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, P.L. 116-283, tit. XCII § 9202 (2021).
[8] Chips and Science Act, P.L. 117-167, div.A, § 106 (2022).
[9] Stefan Pongratz, *Worldwide Telecom Equipment up 3 percent in 2022,* DELL'ORO GROUP (Mar. 16, 2023), https://www.delloro.com/worldwide-telecom-equipment-up-3-percent-in-2022/.
[10] *Public Wireless Supply Chain Innovation Fund*, National Telecommunications and Information Administration (accessed Oct. 17, 2023), https://www.ntia.gov/page/innovation-fund.
[11] "Notice of Funding Opportunity, Public Wireless Supply Chain Innovation Fund Grant Program – Expanding Testing and Evaluation," National Telecommunications and Information Administration (rel. Apr. 12, 2023), https://www.ntia.gov/sites/default/files/publications/pwscif_final_nofo.pdf.
[12] *Biden-Harris Administration Awards Nearly $80M For Wireless Innovation*, National Telecommunications and Information Administration (Jan. 10, 2024), https://www.ntia.gov/press-release/2024/biden-harris-administration-awards-nearly-80m-wireless-innovation.
[13] *Dish Wireless Launches Virtual Open RAN 5G Network with Samsung,* DISH NEWSROOM (Feb. 22, 2023), https://about.dish.com/2023-02-22-DISH-Wireless-Launches-Virtual-Open-RAN-5G-Network-with-Samsung.
[14] *AT&T to Accelerate Open and Interoperable Radio Access Networks (RAN) in the United States through new collaboration with Ericsson,* AT&T (Dec. 4, 2023), https://about.att.com/story/2023/commercial-scale-open-radio-access-network.html.

country.[15] Elsewhere, providers like Rakuten (Japan) and 1&1 (Germany) have already deployed fully O-RAN networks.[16]

3. Rip and Replace

Huawei and ZTE equipment and services are present in American communications networks. These two Chinese telecommunications equipment manufacturers are viewed as threats to communications networks because of their perceived ties to the Chinese government. Specifically, American security officials point to China's 2017 National Intelligence Law, which "requires Chinese companies to support, provide assistance and cooperate in China's national intelligence work, wherever they operate."[17] Further, the opaque ownership structures of these companies raise even more questions of how much influence the Chinese government can assert over them.[18]

To address this threat, Congress enacted the Secure and Trusted Communications Networks Act (STCNA) of 2019.[19] The law prohibits a recipient of the Federal Communications Commission (FCC's) Universal Service Fund (USF) from purchasing, obtaining, or maintaining any equipment or services from companies posing a national security threat, and requires the FCC to publish a list of "covered communications equipment or services" within one year that pose such a threat. The law also established a program to reimburse certain eligible communications providers for replacing covered communications equipment or services. Through the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to the FCC for the reimbursement program.[20]

In July 2022, the FCC announced that a total of $4.98 billion was needed by providers to remove this equipment from U.S. communications networks—a shortfall of $3.08 billion.[21] Absent additional appropriations, the FCC plans to pro-rate each applicant's allocation by 39.5 percent.[22] As of October 2, 2023, reimbursement claim requests have been submitted for 122 of the 126 approved applicants, and these providers have one year from when they submitted their first reimbursement claim to remove untrusted equipment, resulting in deadlines ranging from October 8, 2023, to September 23, 2024.[23] The FCC has approved several requests to extend

---

[15] *Virtualization: What it is and how it's shaping Verizon's 5G network,* VERIZON (May 5, 2023), *https*://www.verizon.com/about/news/virtualization-positioning-our-5g-network-for-the-future.
[16] Nillay Patel, *The risky new way of building mobile broadband networks, explained by Rakuten Mobile CEO Tareq Amin,* THE VERGE (Aug. 9, 2022), https://www.theverge.com/23297756/5g-rakuten-mobile-ceo-oran-cloud-network-decoder.
[17] David E. Sanger et al., *In 5G Race With China, U.S. Pushes Allies to Fight Huawei*, N.Y. Times (Jan. 26, 2019), https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html.
[18] Raymond Zhong, *Who Owns Huawei? The Company Tried to Explain. It Got Complicated.,* N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html.
[19] Secure and Trusted Communications Networks Act of 2019, P.L. 116-124 (2020), *codified at* 47 U.S.C. 1601, et seq.
[20] Consolidated Appropriations Act, 2021 § 906(2).
[21] Letter from Jessica Rosenworcel, Chair, FCC, to Sen. Maria Cantwell et al. (July 15, 2022), https://docs.fcc.gov/public/attachments/DOC-385335A1.pdf.
[22] *Id.*
[23] Letter from Jessica Rosenworcel, Chair, FCC, to Sen. Maris Cantwell et al. (Oct. 10, 2023), https://docs.fcc.gov/public/attachments/DOC-397596A1.pdf.

these deadlines by six months due to the funding shortfall.[24] If this program is not funded before these deadlines, providers who still have this equipment in their networks will no longer be eligible for USF funds,[25] which may lead those providers to shut down affected sites or go out of business.

4. Standard-Setting Organizations

Multi-stakeholder organizations, such as the 3rd Generation Partnership Project (3GPP) and International Telecommunications Union (ITU), are responsible for developing the technical standards for wireless technology. These bodies are generally objective and rely on consensus to reach decisions. China, however, has taken an aggressive approach to participation and leadership in these bodies, overwhelming delegations from the West.[26] As a result, standards could skew in favor of China. However, not all experts view increased Chinese participation as a problem.[27] They point to the open process of deliberations as limiting Chinese influence and argue that engaging China in these forums helps mitigate its threat.[28] Nonetheless, increasing American participation in these bodies could help counter Chinese influence over the process. Congress has focused on enhancing U.S. wireless leadership through efforts to facilitate greater representation of trusted stakeholders at industry standards development bodies and through promoting domestic deployment of trusted wireless solutions. Representative Tim Walberg (R-MI), along with Rep. Debbie Dingell (D-MI), Rep. Bill Johnson (R-OH), and Rep. Ann Kuster (D-NH), have introduced H.R. 1377, the Promoting United States Wireless Leadership Act of 2023, which directs the NTIA to encourage participation of American companies and stakeholders in international standard-setting organizations and offer technical assistance to facilitate that participation.

V. KEY QUESTIONS

- How will O-RAN and V-RAN promote greater supply chain security?
- Is NTIA administering the Innovation Fund effectively?
- How quickly can O-RAN/V-RAN networks get deployed?
- What is the future of O-RAN and V-RAN technology?

VI. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Kate O'Connor or John Lin of the Committee Staff at (202) 225-3641.

---

[24] *Id.*
[25] *See* 47 C.F.R. § 54.9(a) (prohibiting the use of USF support 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).
[26] Valentina Pop, Sha Hua, and Daniel Michaels, From Lightbulbs to 5G, China Battles West for Control of Vital Technology Standards, Wall St. J., Feb. 8, 2021, https://www.wsj.com/articles/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698.
[27] *See* Todd Shields & Alyza Sebenius, *Huawei's Clout is So Strong it's Helping Shape Global 5G Rules*, Bloomberg (Feb. 1, 2019), https://www.bloomberg.com/news/articles/2019-02-01/huawei-s-clout-is-so-strong-it-s-helping-shape-global-5g-rules.
[28] *Id.*