COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

April 19, 2021

To: **Subcommittee on Communications and Technology Members and Staff**
Fr: **Committee on Energy and Commerce Staff**
Re: **Hearing on "Leading the Wireless Future: Securing American Network Technology"**

On **Wednesday, April 21, 2021, at 11:30 a.m.**, the Subcommittee on Communications and Technology will hold a virtual hearing entitled, "Leading the Wireless Future: Securing American Network Technology."

I. BACKGROUND

A. Risks Stemming from Equipment

Some communications service providers have relied heavily on equipment and services manufactured and provided by foreign companies that are not interoperable with equipment from other manufacturers.[1] Today, most wireless carriers construct their communications networks in a given geographic area using equipment from a single manufacturer, which then requires the carriers to purchase other proprietary network components as well.[2] When a network in such an area needs to be upgraded or modified, a carrier must either purchase equipment from the same manufacturer or replace most of the network equipment with that of another manufacturer. There are currently no American companies that manufacture and service this type of end-to-end network equipment, and there are only three non-Chinese companies that do (Nokia, Ericsson, and Samsung).[3]

While large, wireless communications providers with sophisticated network security operations and significant capital generally have avoided installing and using Huawei and other suspect foreign equipment in their networks,[4] smaller carriers with limited resources have; many taking advantage of the deeply discounted prices offered by Huawei and other foreign-government-backed companies, thereby introducing vulnerabilities into U.S. communications

---

[1] U.S.-China Economic Security Review Commission, *Supply Chain Vulnerabilities from China in US Federal Information and Communications Technology* (Apr. 2018).

[2] Brian Fung, *How China's Huawei Took the Lead Over U.S. Companies in 5G Technology*, Washington Post (Apr. 10, 2019) (https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/).

[3] *Id*.

[4] *See, e.g.,* Paul Mozur, *AT&T Drops Huawei's New Smartphone Amid Security Worries,* the New York Times (Jan. 9, 2018) (www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html).

networks.[5] Last year, Congress passed and funded a program to reimburse certain companies for the costs of removing and replacing suspect network equipment and services.[6] Nevertheless, small and large wireless service providers alike still face risks in the acquisition of wireless network equipment due to the relatively small number of companies that can provide an end-to-end network.

New systems of network architecture focused on open interfaces may be able to address such risks. An emerging wireless infrastructure evolution focuses on open network architecture, where the different components of the networks could be produced by different companies (this idea—and the associated technical standards to accomplish this goal—have been dubbed "Open-RAN," standing for Open Radio Access Network).[7] Some have argued that the adoption of Open-RAN, or a similar standard, will allow multiple vendors to provide equipment and services to one network, which in turn may foster competition and support the development of a more diverse, robust, and secure supply chain for network components and services—particularly by trusted vendors—and innovation in wireless networks.[8] Adoption of Open-RAN, however, may also present unique challenges to smaller providers because it would require providers to know how to switch out their own network equipment and ensure that the components are compatible.[9]

Neither the legislation funding the replacement of suspect equipment nor the funding of efforts related to Open-RAN standards focus on consumer equipment integrated into the network. As an increasing number of devices come online driven by surging consumer demand for new connected devices, suspect consumer equipment can create dangerous vulnerabilities in telecommunications networks. These devices can be highjacked by third parties to target other parts of the network infrastructure, exposing the network to risk.[10] Insecure consumer equipment will be an increasing challenge to creating secure telecommunications networks.

---

[5] Wall Street Journal, *State Support Helped Fuel Huawei's Global Rise* (Dec. 25, 2019) (www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736).

[6] Secure and Trusted Communications Networks Act, Public Law No: 116-124; Consolidated Appropriations Act, 2021, Public Law No: 116-260.

[7] Eugina Jordan, *Open RAN 101—Open RAN: Why, What, How, When?*, RCR Wireless (Jul. 1, 2020) (https://www.rcrwireless.com/20200701/opinion/readerforum/open-ran-101-open-ran-why-what-how-when-reader-forum).

[8] ORAN Alliance, *O-RAN Use Cases and Deployment Scenarios*, White Paper (Feb. 2020) (https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5e95a0a306c6ab2d1cbca4d3/1586864301196/).

[9] Iain Morris, *Say Hello to the Open RAN 'Ecosystem,' or Vendor Lock-In 2.0*, Light Reading (Feb. 8, 2021) (https://www.lightreading.com/open-ran/say-hello-to-open-ran-ecosystem-or-vendor-lock-in-20/d/d-id/767225).

[10] Pete Burke, *Protecting critical Internet Infrastructure from IoT Device Risks*, GCN (Dec. 10, 2018) (https://gcn.com/articles/2018/12/10/iot-critical-infrastructure.aspx).

B. Risks Stemming From Spectrum Policy

Within government itself, spectrum management has become increasingly difficult, both due to demands on government spectrum resources as uses of the spectrum proliferate,[11] and because spectrum-using government agencies have sometimes circumvented the statutory spectrum management processes.[12] Congress statutorily tasked the National Telecommunications and Information Administration (NTIA) with managing federal spectrum,[13] but during the past few years, some spectrum-dependent federal agencies have tried to bypass NTIA.[14] Inefficient management and processes ensued, culminating in policy stalemates in several spectrum bands that had previously been identified for shared federal/non-federal use.[15]

II. PREVIOUS CONGRESSIONAL ACTION

In taking action to meet these two challenges, Congress passed the Secure 5G and Beyond Act to enable the President to develop the "Secure Next Generation Mobile Communications Strategy" to ensure the security of 5G communications systems and infrastructure in the United States.[16] Similarly, Congress passed the Secure and Trusted Networks Act to prohibit FCC-administered funds from being used to purchase or support suspect network equipment and services, and to reimburse certain carriers for the cost of replacing suspect network equipment being used in domestic networks.[17] Congress recently funded the reimbursement program at $1.9 billion.[18] Congress also passed the Spectrum IT

---

[11] David Panhans, Rüdiger Schicht, Faisal Hamady, and Thibault Werlé, *The Coming Battle for Spectrum*, BCG (Feb. 11, 2020) (https://www.bcg.com/publications/2020/coming-battle-for-spectrum).

[12] *See, e.g.*, Letter from Assistant Secretary Jim Blew, U.S. Department of Education, to Secretary Marlene H. Dortch, Federal Communications Commission, re: *Transforming the 2.5 GHz Band, WT Docket No. 18-120* (June 7, 2019); Letter from Assistant Secretary Bruce Walker, U.S. Department of Energy, to Chairman Ajit Pai, Federal Communications Commission (Sept. 3, 2019) (regarding the 6 GHz spectrum band); Letter from Acting Secretary, Department of Defense, to Chairman Ajit Pai, Federal Communications Commission (June 7, 2019), and Letter from Secretary Mark Esper, U.S. Department of Defense, to Chairman Ajit Pai, Federal Communications Commission (Nov. 18, 2019) (letters regarding GPS signal concerns).

[13] National Telecommunications and Information Administration Organization Act, PL 102–538, Oct. 27, 1992, as amended by PL 115–141, Mar. 23, 2018 (codified at 47 USC § 901 et seq.); *see also* National Telecommunications and Information Administration, *Spectrum Management*, www.ntia.doc.gov/category/spectrum-management (last visited Jan. 1, 2020). *See also*, 47 USC §§ 305, 902.

[14] *See* note 2.

[15] Letter from Rep. Frank Pallone, Jr., Chairman, and Greg Walden, Ranking Member, House Committee on Energy and Commerce, to Gene L. Dodaro, Comptroller General of the United States (Jan. 24, 2020).

[16] Secure 5G and Beyond Act, Public Law No: 116-129.

[17] Secure and Trusted Communications Networks Act, Public Law No: 116-124.

[18] Consolidated Appropriations Act, 2021, Public Law No: 116-260.

Modernization Act, which will allow the federal government to improve coordination by updating and streamlining its spectrum management infrastructure.[19]

III. ONGOING CONGRESSIONAL ACTION

Last year, Congress passed the Utilizing Strategic Allied (USA) Telecommunications Act of 2020 to award grants to support the deployment of Open-RAN 5G Networks throughout the United States.[20] However, the Act has not yet been funded. Congress is currently considering how to fund it and for how much. Recently, a bipartisan group of senators requested that President Biden put $3 billion toward funding Open-RAN, so that equipment vendors can compete in the 5G market with Huawei and ZTE.[21] The money would go into the Public Wireless Supply Chain Innovation Fund and the Multilateral Telecommunications Security Fund ($1.5 billion in each), which were created in the 2021 National Defense Authorization Act.[22] Likewise, research and development efforts are being considered in the Senate through Senator Schumer's Endless Frontiers Act,[23] which would increase federally-funded research and development to achieve national goals related to economic competitiveness, domestic manufacturing, national security, including in the area of advanced communications technology, among other areas.[24] Additional issues have not yet been addressed by Congress, including helping smaller providers with technical assistance and securing consumer equipment.

IV. WITNESSES

The following witnesses have been invited to testify:

John Baker
Senior Vice President, Business Development
Mavenir

John Mezzalingua
Chief Executive Officer
JMA Wireless

---

[19] The Spectrum IT Modernization Act became part of the National Defense Authorization Act (NDAA) for Fiscal Year 2021, Public Law No: 116-283.

[20] The USA Telecommunications Act became part of the 2021 NDAA, Public Law No: 116-283.

[21] John Eggerton, *Senators Ask Biden for $3 Billion for ORAN Alternative to Chinese Tech*, Next TV (Apr. 6, 2021) (https://www.nexttv.com/news/senators-ask-biden-for-dollar3-billion-for-oran-alternative-to-chinese-tech).

[22] *Id*.

[23] S. 3832, 116th Cong. (2020).

[24] The National Law Review, *The Endless Frontier Act: Shifting the Focus from Defense to Offense* (Apr. 15, 2021) (https://www.natlawreview.com/article/endless-frontier-act-shifting-focus-defense-to-offense).

Tim Donovan
SVP, Legislative Affairs
Competitive Carriers Association

Tareq Amin
EVP and Group Chief Technology Officer
Rakuten Mobile

Diane Rinaldo
Executive Director
Open RAN Policy Coalition