COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

June 25, 2021

To: Subcommittee on Communications and Technology Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Legislative Hearing on "A Safe Wireless Future: Securing our Networks and Supply Chains"

On **Wednesday, June 30, 2021, at 10:30 a.m., in the John D. Dingell Room, 2123 of the Rayburn House Office Building, and via Cisco WebEx online video conferencing,** the Subcommittee on Communications and Technology will hold a legislative hearing entitled, "A Safe Wireless Future: Securing our Networks and Supply Chains."

I. BACKGROUND

As consumer demand drives an increasing number and diversity of wireless devices, the United States faces converging security, supply chain, and other policy issues related to wireless networks. For example, vulnerable internet of things devices can be highjacked by third parties to target other parts of the network infrastructure, exposing networks to risk.[1] Wireless networks can also be exposed to risk by their own network components.[2] For instance, some communications service providers have relied heavily on equipment and services manufactured and provided by non-trusted companies that are not interoperable with equipment from other manufacturers.[3] Clarifying governance responsibilities with regard to network security is critical in the face of these new risks to ensure the United States can mount coordinated and efficient responses to security incidents and also identify new risks.[4] The United States is engaged in a global race to produce innovative new wireless technologies, lest the nation be

[1] 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).

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

[3] *Id*.

[4] Charlie Mitchell, *Former FCC Security Chief Simpson: To Secure 5G, Clarify Roles and Responsibilities, Offer Incentives*, Inside Cybersecurity (insidecybersecurity.com/daily-news/former-fcc-security-chief-simpson-secure-5g-clarify-roles-and-responsibilities-offer) (Mar. 17, 2020).

relegated to relying on suspect equipment, technologies, or services.[5] These issues, though distinct in key ways, are intertwined and collectively, they have national security implications.[6]

In recent years, Congress has taken numerous actions aimed at mitigating converging supply chain and security risks. With regard to securing our networks, Congress passed and funded a program to reimburse certain companies for the costs of removing and replacing suspect network equipment and services.[7] Congress also passed legislation to create a national 5G Security Strategy, but risks continue to evolve.[8] Congress has also authorized the Public Wireless Supply Chain Innovation Fund to promote and deploy open interfaced network technologies.[9] While that program has yet to be funded, stakeholders still require solutions regarding how best to help small providers diversify their supply chains, in appropriate circumstances, and secure end user equipment.[10]

II. LEGISLATION

A. H.R. 2685, The "Understanding Cybersecurity of Mobile Networks Act"

On April 20, 2021, Reps. Eshoo (D-CA) and Kinzinger (R-IL) introduced H.R. 2685, the Understanding Cybersecurity of Mobile Networks Act. The bill would require the National Telecommunications and Information Administration (NTIA) to examine and report on the cybersecurity of mobile service networks and the vulnerability of these networks and mobile devices to cyberattacks and surveillance conducted by adversaries. The report must include an assessment of the degree to which providers of mobile service have addressed certain cybersecurity vulnerabilities; a discussion of the degree to which these providers have implemented cybersecurity best practices and risk assessment frameworks; and an estimate of the prevalence and efficacy of encryption and authentication algorithms and techniques used in mobile service and communications equipment, mobile devices, and mobile operating systems and software, among other things.

---

[5] *Id*.

[6] *Id*.

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

[8] Secure 5G and Beyond Act, Pub. L. No. 116-129.

[9] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, Sec. 9202.

[10] House Committee on Energy and Commerce, *Leading the Wireless Future: Securing American Network Technology*, 117th Cong. (2021).

B. H.R. 3919, the "Secure Equipment Act of 2021"

On June 15, 2021, Reps. Scalise (R-LA) and Eshoo introduced H.R. 3919, the Secure Equipment Act of 2021. The bill would direct the Federal Communications Commission (FCC) to clarify that it will no longer review or approve applications from companies on the Commission's "Covered List," required under the Secure and Trusted Communications Networks Act (STCNA). The bill would prevent further integration and sales of Huawei, ZTE, Hytera, Hikvision, and Dahua – all Chinese state-backed or directed firms – in the United States regardless of whether federal funds are involved.

C. H.R. 4028, the "Information and Communication Technology Strategy Act"

On June 22, 2021, Reps. Long (R-MO), Spanberger (D-VA), Carter (R-GA), and McNerney (D-CA), introduced H.R. 4028, the Information and Communication Technology Strategy Act. The bill would direct the Secretary of Commerce to submit to Congress within one year a report analyzing the state of economic competitiveness of trusted vendors in the information and communication technology supply chain, identify which components or technologies are critical or vulnerable, and identify which components or technologies U.S. networks depend upon. It would also require the Secretary to submit to Congress, within six months after the report is submitted, a whole-of-government strategy to ensure the competitiveness of trusted vendors in the United States.

D. H.R. 4029, the "Timely Evaluation of Acquisitions, Mergers, or Transactions with External, Lawful Entities to Clear Owners and Management Act" (THE ''TEAM TELECOM" ACT)

On June 22, 2021, Rep. Johnson (R-OH) introduced H.R. 4029, the TEAM TELECOM Act. The bill would formalize the existing review process for entities applying for authorization to construct or extend any transmission line or submarine cable line where the applicant has above a certain threshold of foreign ownership interest. This bill would put NTIA in charge of the coordinating efforts with appropriate federal agencies with subject matter expertise.

E. H.R. 4032, the "Open RAN Outreach Act"

On June 22, 2021, Reps. Allred (R-TX), O'Halleran (D-AZ), Hudson (R-NC), and Guthrie (R-KY) introduced H.R. 4032, the Open RAN Outreach Act. The bill directs the NTIA Administrator to provide outreach and technical assistance to small communications network providers regarding Open Radio Access Networks (Open-RAN).

F. H.R. 4045, the "Future Uses of Technology Upholding Reliable and Enhanced Networks Act" (THE "FUTURE Networks" ACT)

On June 22, 2021, Reps. Doyle (D-PA), Johnson and McBath (D-GA), introduced H.R. 4045, the FUTURE Networks Act. This bill would require the FCC to create a 6G (sixth-generation) Task Force. The bill stipulates that the membership of the Task Force shall be appointed by the FCC Chair, and that the membership composition of the Task Force should be composed, if possible, of representatives from trusted companies (meaning those not controlled by foreign adversaries), trusted public interest groups, and trusted government representatives with at least one representative from federal, state, local, and tribal governments. The Task Force would have to submit a report to Congress on 6G wireless technology, including the

possible uses, strengths, and limitations of 6G (including any supply chain, cybersecurity, or other limitations that will need to be addressed in future generations of wireless technologies).

G. H.R. 4046, the "NTIA Policy and Cybersecurity Coordination Act"

On June 22, 2021, Reps. Duncan (R-SC) and Wild (D-PA) introduced H.R. 4046, the NTIA Policy and Cybersecurity Coordination Act. The bill would authorize the existing NTIA office of Policy Analysis and Development and rename it the Office of Policy Development and Cybersecurity. In addition to codifying the responsibilities of NTIA in administering the STCNA Section 8 information sharing program, the Office would be assigned functions to coordinate and develop policy regarding the cybersecurity of communications networks.

H. H.R. 4055, the "American Cybersecurity Literacy Act"

On June 22, 2021, Reps. Kinzinger, Eshoo, Veasey (D-TX) and Houlahan (D-PA) introduced H.R. 4055, the American Cybersecurity Literacy Act. The bill would require NTIA to develop and conduct a cybersecurity literacy campaign to educate U.S individuals and businesses about common cybersecurity risks and best practices.

I. H.R. 4067, the "Communications Security Advisory Act of 2021"

On June 22, 2021, Reps. Slotkin (D-MI), Schrader (D-OR) and Walberg (R-MI) introduced H.R. 4067, the Communications Security Advisory Act of 2021. The bill would codify an existing FCC advisory council, the Communications Security, Reliability, and Interoperability Council, focused on network security, resiliency, and interoperability. It also requires biennial reporting to the FCC, Congress, and public with recommendations to improve communications networks on such issues.

III. WITNESSES

The following witnesses have been invited to testify:

Dileep Srihari
Senior Policy Counsel
Access Partnership

Dean Brenner
SVP, Spectrum Strategy & Tech Policy
Qualcomm Incorporated

Jason Boswell
Head of Security, Network Product Solutions, N.A.
Ericsson

Clete Johnson
Senior Fellow, Strategic Technologies Program
Center for Strategic and International Studies