U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

May 14, 2018

TO: Members, Subcommittee on Communications and Technology

FROM: Committee Majority Staff

RE: Hearing entitled "Telecommunications, Global Competitiveness, and National Security."

I. INTRODUCTION

The Subcommittee on Communications and Technology will hold a hearing on Wednesday, May 16, 2018, at 10:00a.m. in 2123 Rayburn House Office Building. The hearing is entitled "Telecommunications, Global Competitiveness, and National Security."

II. WITNESSES

- Dr. Charles Clancy, Director and Professor, Hume Center for National Security and Technology, Virginia Tech;
- Ms. Samm Sacks, Senior Fellow, Technology Policy Program, Center for Strategic and International Studies; and,
- Mr. Clete Johnson, Partner, Wilkinson Barker Knauer, LLP.

III. BACKGROUND

Closing the digital divide as long been a priority of the Subcommittee on Communications and Technology. The Subcommittee's focus on expanding broadband access in a technologically neutral manner, promoting competition in both the wireline and wireless markets, and protecting our telecommunications infrastructure from national security threats is an essential part of driving the economic engine and improving consumers' online experience.[1] When threats to the competition or national security of the telecommunications industry arise, it directly thwarts our ability to achieve these goals.[2] This hearing seeks to better understand these

[1] U.S. House of Representatives, Committee on Energy and Commerce hearing entitled, "Closing the Digital Divide: Broadband Infrastructure Solutions." January 30, 2018 (115th Congress). Information available at: https://energycommerce.house.gov/hearings/closing-digital-divide-broadband-infrastructure-solutions/

[2] U.S. House of Representatives, Committee on Energy and Commerce hearing entitled, "An Examination of the Communications Supply Chain." May 21, 2013 (113th Congress). Information available at https://energycommerce.house.gov/hearings/cybersecurity-examination-communications-supply-chain/

threats to competition and national security, the prevalence of troublesome equipment in U.S. telecommunications networks, and the U.S. Government and industry's response to these threats.

When examining threats to the telecommunications industry, it is critical to evaluate every node in the supply chain. For example, within the networks, there are various primary and secondary suppliers that provide the different layers of the network, including the physical layers,[3] logical network routing functions,[4] and the software-based application layers.[5] Within the devices, there are semiconductors, memory capacity, and other microelectronics that are necessary to the device's function. Finally, many equipment providers also include ongoing services like network management, technician support, repair and replacement of parts, and billing. Vulnerabilities posed by some equipment and services, like the ability of foreign actors to deliberately inject an exploit into a node in the network, and our ability—or inability—to mitigate such threats are concerning.

Additionally, there are longer-term threats to the vendor landscape. Telecommunications providers must weigh the tradeoffs between purchasing economical equipment versus more expensive brands. Some providers have access to sensitive national security information through information sharing mechanisms with the Federal government that help inform these decisions, but other, generally smaller providers do not.[6] Moreover, threats to competition in vendor markets can leave U.S. telecommunications providers vulnerable to potentially at-risk equipment with no alternatives. Some actors, for example, seek to dominate specific nodes in the supply chain, leaving the rest of the world dependent on them for critical components.

a. Prevalence and Pervasiveness of Vulnerable Equipment in U.S. Telecommunications Networks

Today, much of the vulnerable equipment we are discussing is found in rural America, predominantly in the networks of smaller providers. Due to the economic factors that increase costs to provide broadband in rural areas, many of these providers depend on support they receive from the Federal Communications Commission's Universal Service Fund (USF). By accepting USF support, these providers must efficiently use Federal funds. USF support, along with other economic factors that drive costs, lead many of these providers to purchase equipment or services from vendors at below-market costs. It is estimated that vulnerable equipment makes up less than one percent of the equipment in American cellular and landline networks.[7]

---

[3] This generally refers to layers 1 and 2 of the OSI model; *See*, majority memorandum from hearing entitled, "From Core to Edge: Perspective on Internet Prioritization." at pp. 2-3. Available at: https://docs.house.gov/meetings/IF/IF16/20180417/108168/HHRG-115-IF16-20180417-SD002-U2.pdf

[4] *Supra*, note 3, at 3-4. This generally refers to layers 3-4 of the OSI model.

[5] *Supra*, note 3, at 3-4. This generally refers to layers 5-7 of the OSI model.

[6] See, National Cybersecurity and Communications Integration Center (NCCIC), U.S. Department of Homeland Security. Information available at: https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[7] Drew FitzGerald and Stu Woo, "In U.S. Brawl with Huawei, an Unlikely Loser: Rural Cable Firms," Wall Street Journal (3/27/18), https://www.wsj.com/article/caught-between-two-superpowers-the-small-town-cable-guy-1522152000.

Even if penetration of our domestic telecommunications equipment market is less than one percent, the Subcommittee remains cognizant of the global nature of the equipment market, and that this market is characterized by scale. Thus, if vendors of vulnerable equipment are banned from the U.S. market, how long can trusted vendors compete over the long term? Moreover, even if it is possible for rural networks to mitigate threats, there remains a larger issue about the Internet itself as a global network of networks; some traffic will inevitably ride over a foreign network and foreign data packets will inevitably transit our domestic networks. This fact illustrates the difficulty of securing U.S. networks and supply chains.

b. Questions to be Considered

Threats to National Security

In the immediate term, threats to the telecommunications supply chain exist both in the hardware deployed throughout our networks and the software used to manage those networks – as well as in the software in the devices used to connect to our networks. These devices not only include mobile handsets, but also Internet of Things (IoT) devices, smart-home devices, and smart-home appliances. Though the nature of these threats is usually classified, we seek to understand in an open setting the immediate risks to our networks.

To this end, the committee will examine the role of standards bodies, which set the rules for equipment providers and suppliers. Standards bodies have immense power in shaping the technical foundations of networks and devices. To what extent can nefarious actors influence these technical standards for an asymmetric advantage? To what extent can trusted vendors use standard setting bodies to negate or otherwise minimize the influence of nefarious actors? While some companies heavily invest in their standards teams, does sending dozens to hundreds of their employees to standards bodies ensure fair, equitable, and technologically sound outcomes? Should the U.S. establish appropriate transparency and standardized mechanisms to resolve these issues? Is there a role for government, or should industry stakeholders determine the means to collaborate with international partners?[8]

The Subcommittee will also consider risk management-based approaches to network security threats. Risk management entails a multi-step process of threat mitigation that focuses on the most critical components first, and then expands to other, less critical parts of the network. Is it sufficient to have awareness in vendor decisions across some or all corners of an organization – from procurement and acquisition to installation and cybersecurity? What role does information sharing between the Federal government and the private sector help optimize security? Should we forgo risk management in favor of proposals to "rip and replace" vulnerable equipment? Is there a risk of a "whack-a-mole" scenario in which providers "rip" vulnerable equipment out of the network and "replace" it with new equipment later, only to discover later that it, too, has cyber vulnerabilities?

[8] See, "Industry Leaders Launch ORAN Alliance." Available at: http://about.att.com/story/industry_leaders_launch_oran_alliance.html

Threats to Competition

Though the immediate threats to national security usually garner more attention, there are equally concerning longer-term threats to global competition. As we look to close the digital divide and win the race to develop 5G, we need to ensure the U.S. remains a globally competitive leader. A proactive, long-term approach includes evaluating our domestic manufacturing capacity, the open-nature of our investment policy, and our engagement in standards-setting bodies. To that extent, the Subcommittee will explore the broader implications beyond mitigating immediate threats to our communications networks. If component pieces are produced in the U.S., but the manufacturing or assembly process occurs in foreign states, would there be long-term vulnerabilities in the supply chain industries, component pieces, or networking and device gear?

Does the open nature of our investment environment potentially leave us at a competitive disadvantage? Do transactions that leave foreign investors in control of vendors in strategic positions in the supply chain pose long term threats to competition? Since the Information and Communications Technology (ICT) supply chain is truly global, do we need capacity to manufacture this equipment domestically? Is it vital to U.S. competitiveness on a global scale that we have a long-term strategy to address the dwindling vendor landscape, reliable access to critical raw materials and component pieces, and the manufacturing capability to lessen dependence on foreign equipment? China has developed a long-term plan—the Made in China 2025 Initiative—to no longer be restrained by others for core technologies in strategically competitive fields and has prioritized projects around core electronic equipment, high-end universal chips, basic software, large-scale IC, next-generation wireless broadband mobile communication, quantum communication, and quantum computing.[9] Should the United States do the same? What are the implications of these factors on the race to 5G?

In the same vein, what are the implications in the race to develop and deploy super- and quantum-computing capabilities and quantum communications on a wide scale? Early analysis suggests that when it comes to quantum computing and quantum communications, the U.S. has shown interest in building the hardware, and China and Japan have been more focused on the applications, software, and use-cases.[10] Global competition in the early stages of this race will shape the vendor landscape in future years when quantum communications may have commercial applications. Will competitively developing our own systems position us to tackle threats to competition as the technology develops?

c. U.S. Government Response

FCC Response

---

[9] Samm Sacks, "Beijing's Cyber Governance System." *Meeting the China Challenge: Responding to China's Managed Economy*, CSIS, at 36. (January 2018) Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180126_Lewis_MeetingChinaChallenge_Web.pdf?ccS38O06FR8XG_yUn7GS1YrJXOTCZklM

[10] *See*, https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race

On April 17, 2018, the FCC adopted a Notice of Proposed Rulemaking (NPRM) examining the role of the FCC in protecting the nation's communications supply chain against national security threats.[11] Specifically, the NPRM seeks comment on a proposed rule that would restrict telecommunications providers from using support from the universal service fund (USF) to purchase or obtain 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. In addition to restricting USF-funded equipment or services, the NPRM also asks whether the FCC should take action towards non-USF-funded equipment or services produced or provided by companies that might post national security threats to the nation's communications networks.

While the NPRM would apply the rule on a prospective basis, it seeks comment on the degree to which equipment and services that might pose a threat are deployed in *existing* networks, particularly by small and rural carriers. Further, the NPRM seeks comment on the potential costs to further expanding broadband to unserved or underserved areas if the goal of ensuring national security in the supply chain is achieved. This is particularly relevant as policymakers consider development of 5G networks. The FCC has also considered national security concerns in other contexts, including in the course of reviewing applications under section 214 and in re-chartering the Communications Security, Reliability and Interoperability Council (CSRIC), which is charged with providing recommendations to ensure the security and reliability of the nation's communications systems.[12]

Department of Commerce Response

Recently, the Department of Commerce examined the role of technology transfers within the telecommunications industry—specifically the oversight of these transfers. Technology transfers, broadly speaking, are the dissemination of technology across international borders. Foreign actors that have asymmetric advantages over the United States in technological prowess can use that information not only to introduce threats to our networks, but also to create their own products that rival or outcompete domestically sourced suppliers.

There are several mechanisms in place across the Federal government to address threats posed by technology transfers. Team Telecom, for example, is a working group of national security officials across the Federal government that reviews transactions for national security vulnerabilities.[13] Additionally, the Federal government reviews transactions where foreign entities take a majority ownership stake in U.S. companies. In addition, the Committee on Foreign Investment in the United States (CFIUS) is, "an inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person, in order to

[11] Federal Communications Commission, Notice of Proposed Rulemaking, "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs." (WC Docket No. 18-89), FCC 18-42, Adopted April 17, 2018. Available at: https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0418/FCC-18-42A1.pdf

[13] Team Telecom has representatives from the Departments of Homeland Security, Defense, Justice, State, Treasury, and Commerce, as well as the U.S. Trade Representative and the Federal Bureau of Investigation.

determine the effect of such transactions on the national security of the United States."[14] The Department of Commerce holds a voting seat on both of these entities.[15]

As the Department of Commerce addresses these issues, the National Telecommunications and Information Administration (NTIA) coordinates the Federal government response. NTIA coordinates the response to threats to national security with industry stakeholders. In doing so, NTIA works closely with the National Institute of Standards and Technology (NIST) to help industry stakeholders apply the cybersecurity framework to their networks and mitigate potential threats to national security. The standards and best practices from an engineering standpoint that NIST develops directly inform the response to these threats. Also within the Department of Commerce is the Bureau of Industry and Security (BIS), which addresses external threats posed by foreign actors, including technology transfers. BIS recently issued an order activating the denial of export privileges of Zhongxing Telecommunications Equipment Corporation (ZTE).[16]

National Defense Authorization Act for Fiscal Year 2019

There are several aspects regarding the Fiscal Year 2019 National Defense Authorization Act (NDAA) that relate to telecommunications, global competitiveness, and national security.[17] Chiefly, section 866(b) would prohibit Federal agencies from contracting with "covered telecommunications providers", which are explicitly named and limited to Huawei Technology Corporation, ZTE Corporation, or any subsidiary, successor entity, or affiliate.[18] The Subcommittee will examine whether the definition of "covered telecommunications equipment or services" could be interpreted to include all domestic telecommunications providers and, if so, how it affect Federal agencies' ability meet their communications needs.

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Sean Farrell, Tim Kurth, or Robin Colwell of the Committee Staff at (202) 225-2927.

---

[14] *See*, https://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx
[15] *Supra*, notes 13 and 14.
[16] U.S. Department of Commerce, Bureau of Industry and Security, "Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd." April 15, 2018. Available at: https://www.commerce.gov/sites/commerce.gov/files/zte_denial_order.pdf
[17] H.R. 5515, Chairman's Mark. Available at: https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/wysiwyg_uploaded/FY19%20NDAA%20Chairman%27s%20Mark%20Final.pdf
[18] *Supra*, note 19, at Sec. 866(b)(4)(D).