MEMORANDUM 2/13/2024

To: Members, Subcommittee on Communications and Technology
From: Majority Staff
Re: Communications and Technology Subcommittee Hearing

I. INTRODUCTION

On Thursday, February 15, 2024, at 10:00 a.m. (ET), the Subcommittee on Communications and Technology will hold a hearing in 2123 Rayburn House Office Building titled "Securing Communications Networks from Foreign Adversaries." The following witnesses are expected to testify:

II. WITNESSES

- Mr. James Lewis, Senior Vice President, Center for Strategic and International Studies (CSIS)
- Mr. Craig Singleton, China Program Senior Director and Senior Fellow, Foundation of Defense of Democracies
- Ms. Lindsay Gorman, Senior Fellow for Emerging Technologies, German Marshall Fund's Alliance for Securing Democracy

III. BACKGROUND

In recent decades, the Chinese Communist Party (CCP) has taken aggressive steps to overtake the United States and its allies as the world's economic power.[1] The CCP invested heavily into a range of industries domestically to become less dependent on the United States and its allies for China's critical infrastructure.[2] In the case of communications infrastructure, the CCP developed unsecure telecommunications equipment and exported it around the world in order to assist in its espionage activities.[3] Congress passed the Secure and Trusted

---

[1] Matthew Reynolds, *Standing United Against the People's Republic of China's Economic Aggression and Predatory Practices,* Center for Strategic & International Studies (May 18, 2023), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-05/ts230517_Reynolds_Economic_Aggression.pdf?VersionId=xNi8qfzihhppiwXpriMd5uRUrzdpXFH2.

[2] Anshu Siripuranu and Noah Berman, *The Contentious U.S.-China Relationship,* Council on Foreign Relations (Sept. 26, 2023), https://www.cfr.org/backgrounder/contentious-us-china-trade-relationship.

[3] *A Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, Permanent Select Committee on Intelligence*, U.S. House of Representatives 112th (Oct. 8, 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

Communications Networks Act of 2019 to remove some of this equipment from networks in the United States and help carriers replace it with equipment from trusted vendors.[4]

Americans rely on technology daily for some of their most personal needs, such as banking, healthcare, or communications. As Americans become more connected, it becomes even more crucial that the equipment that they buy is secure. With the known vulnerabilities in many technologies produced by the CCP, we must take steps to reduce the widespread availability of this equipment that poses a national security threat in the United States.[5]

IV. SELECTED ISSUES

Chinese Communist Party Influence

American officials note that the "increasingly authoritarian nature of the CCP, the fading line between independent business and the state and new laws that will give Beijing the power to look into, or maybe even take over, networks that companies like Huawei have helped build and maintain."[6] Specifically, they 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," which could implicate equipment they sell in the United States.[7] Further, the opaque ownership structures of Chinese companies raise even more questions of how much influence the Chinese government can assert over them, leading to uncertainty about the national security threats posed by Chinese technology. [8]

Supply Chain Security

On Mach 12, 2020, Congress enacted the Secure and Trusted Communications Networks Act (STCNA) of 2019.[9] The law prohibits a Universal Service Fund (USF) recipient 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, which includes CCP owned companies, including Huawei and ZTE.[10] The law also established a program to reimburse eligible communications providers for replacing covered communications equipment or services. Through the Consolidated Appropriations Act, 2021, Congress provided $1.9 billion to the

---

[4] Secure and Trusted Communications Networks Act of 2019, P.L. 116-124 (2020), codified at 47 U.S.C. 1601, et seq.
[5] *The China Threat,* The Federal Bureau of Investigation (accessed Feb. 8, 2024), https://www.fbi.gov/investigate/counterintelligence/the-china-threat.
[6] 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.
[7] *Id.*
[8] 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.
[9] *Supra* note 4.
[10] *List of Equipment and Services Covered by Section 2 of The Secure Networks Act,* The Federal Communications Commission (accessed Feb. 8, 2024), https://www.fcc.gov/supplychain/coveredlist.

Federal Communications Commission (FCC) for the reimbursement program.[11] Demand for this program exceeded the initial estimate, resulting in a shortfall of $3.08 billion.[12]

On November 11, 2021, Congress enacted the Secure Equipment Act into law. The Secure Equipment Act requires the FCC to adopt rules to update its equipment authorization procedures to no longer consider any applications for equipment that is on the list of covered communications equipment and services published by the FCC pursuant to section 2(a) of STCNA. The FCC adopted rules on November 25, 2022.[13]

Taiwan Undersea Cables

Undersea cables are responsible for carrying data traffic across oceans. There are 574 active and submarine cable systems that keep the world connected.[14] Taiwan depends on fourteen submarine cables to keep it connected to the global internet.[15] These cables are at risk amid rising tensions with China. In February, a Chinese fishing vessel cut the two undersea cables connecting Taiwan's Matsu islands to the Taiwan's main island, disconnecting the 14,000 people who live there from the internet.[16] In response, Taiwan is working to secure its connectivity, including by adding new cables and looking at alternative technologies, including satellite and cloud solutions.[17]

V. LEGISLATION

The Subcommittee on Communications and Technology intends to discuss the following legislation.

1. H.R. 2864, the Countering CCP Drones Act (Rep. Elise Stefanik)

H.R. 2864 was introduced by Representative Elise Stefanik (R-NY) on April 25, 2023. The bill would amend the Secure and Trusted Communications Networks Act to provide for the addition of certain equipment and services provided or provided by DJI Technologies to the list of covered communications equipment or services published. Under the Secure and Trusted

---

[11] Consolidated Appropriations Act, 2021 § 906(2).
[12] Letter from Jessica Rosenworcel, Chair, FCC, to the Hon. Maria Cantwell et al. (July 15, 2022), https://docs.fcc.gov/public/attachments/DOC-385335A1.pdf.
[13] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232 et al., Report and Order, Order, and Further Notice of Proposed Rulemaking, FCC 22-84 (rel. Nov. 25, 2022), https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf.
[14] *Submarine Cable Frequently Asked Question*, TeleGeography (Feb 8. 2024), https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.
[15] Chung Li-hua and Jonathan Chin, *Taiwan to add subsea Internet Cables,* Taipei Times (Apr. 16, 2023), https://www.taipeitimes.com/News/front/archives/2023/04/16/2003798023.
[16] Sarah Wu and Yimou Lee, *Fear of the dark: Taiwan sees wartime frailty in communication links with world,* Reuters (Mar. 15, 2023), https://www.reuters.com/world/asia-pacific/fear-dark-taiwan-sees-wartime-frailty-communication-links-with-world-2023-03-15/
[17] Id.

Communications Networks Act, covered communications equipment or services pose an unacceptable risk to national security.

2. H.R. 820, the Foreign Adversary Communications Transparency Act (Rep. Elise Stefanik)

H.R. 820 was introduced by Representative Elise Stefanik (R-NY) on February 2, 2023. The bill would require the FCC to publish annually a list of entities that hold a license or other authorization granted by the FCC and have ties to specified countries. An entity must be listed if the government of China, Cuba, Iran, North Korea, Russia, or Venezuela (or an organization subject to the jurisdiction of any of those governments) owns an equity interest in the entity. The FCC may list additional entities that do not meet these requirements after consulting with an appropriate national security agency.

3. H.R. 1513, the Future Uses of Technology Upholding Reliable and Enhancing Networks (FUTURE Networks) Act (Rep. Doris Matsui)

H.R. 1513 was introduced by Representative Doris Matsui (D-CA) on March 9, 2023. The bill would require the FCC to establish a 6G Task Force to develop a report on sixth-generation wireless technology, including the status of the standards development and possible uses of such technology. The task force shall be composed of representatives from trusted companies in the communications industry, trusted public interest organizations or academic institutions, and federal, state, local, and tribal governments.

4. H.R.___, the Promote Secure Connectivity to Taiwan Act

The discussion draft would direct the National Telecommunication and Information Administration (NTIA) to submit to Congress a report containing an assessment of technologies available to increase the security and resiliency of the communications networks of Taiwan, including through assessing engagement with trusted entities, existing communications infrastructure, and the need for such technologies.

5. H.R.___, Removing Our Unsecure Technologies to Ensure Reliability and Security (ROUTERS) Act

The discussion draft would require the Assistant Secretary for Communications and Information at the Department of Commerce to conduct a study of the national security risks posed by routers, modems, or devices that combine both, that are designed, developed, manufactured, or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of the People's Republic of China, Russia, Iran, North Korea, Cuba, or Venezuela.

VI. KEY QUESTIONS

- What are the key vulnerabilities in communications that foreign adversaries exploit?

- Is the U.S. positioning itself and its allies to incentivize secure vendors of communications equipment?
- Are there specific pieces of communications equipment that are critical to securing U.S. networks?

VII. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Kate O'Connor, Giulia Leganski, John Lin, or Slate Herman of the Committee Staff at (202) 225-2927.