GREG WALDEN, OREGON
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FIFTEENTH CONGRESS

Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

MEMORANDUM

May 14, 2018

To: Subcommittee on Communications and Technology Democratic Members and Staff

Fr: Committee on Energy and Commerce Democratic Staff

Re: Hearing on "Telecommunications, Global Competitiveness, and National Security"

On **Wednesday, May 16, 2018, at 10:00 a.m. in room 2123 of the Rayburn House Office Building,** the Subcommittee on Communications and Technology will hold a hearing titled "Telecommunications, Global Competitiveness, and National Security."

I. BACKGROUND

Communications networks in the United States increasingly rely on equipment and services manufactured and provided by foreign companies. According to the Government Accountability Office (GAO), more than 100 foreign countries imported communications network equipment into the U.S. market between 2007 and 2011.[1] While the globalization of commerce and trade has created many benefits, these long supply chains have made it possible for bad actors to exploit vulnerabilities during design, production, delivery, and post-installation servicing. The National Counterintelligence Executive has noted that "the globalization of the economy has placed critical links in the manufacturing supply chain under the direct control of U.S. adversaries."[2]

Some examples of communications supply chain threats include: (1) attempts to disrupt the ability of an organization to operate on the Internet; (2) attempts to infiltrate a computer system to view, delete, or modify data, and; (3) attempts to use viruses or worms to extract data

[1] U.S. Government Accountability Office, *Telecommunications Networks: Addressing Potential Risks of Foreign-Manufactured Equipment* (May 21, 2013) (GAO-13-301).

[2] Office of the National Counterintelligence Executive, *Supply Chain Threats* (www.ncix.gov/issues/supplychain/index.php).

for use or sale. Some experts have even expressed concerns about the use of a "kill switch," which could cause widespread communications outages and interruption of the power grid.[3]

In October 2012, the House Permanent Select Committee on Intelligence released a report concluding that Chinese telecommunications companies Huawei and ZTE "pose a security threat to the United States."[4] The report encouraged U.S. companies to take into account the long-term security risks associated with Huawei and ZTE and recommended that U.S. government systems, particularly sensitive systems, exclude equipment and component parts, manufactured by those companies. More recently, a report commissioned by the U.S.-China Economic Security Review Commission found that the Chinese government has "invested significant state capital and influence" on state-owned enterprises in order to strategically place these companies in the U.S. telecom supply chain.[5]

II. RECENT FEDERAL ACTIONS

A. FCC Notice of Proposed Rulemaking

The Federal Communications Commission (FCC) released an item proposing to prohibit Universal Service Fund (USF) payments to purchase "equipment or services produced or provided by a company that presents a risk to the supply chain."[6] In the Notice of Proposed Rule Making (NPRM), the FCC seeks comments on a number of questions posed by such a ban, including the types of equipment and services that should be covered by the prohibition, how the proposed prohibition would affect multi-year contracts, and how to identify the parties that pose a national security risk to U.S. communications systems.

B. BIS Denial of Export Privileges Against ZTE

On April 16, 2018, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced that it had imposed a seven-year denial of export privileges against ZTE, effectively banning U.S. companies from selling components to the company, for false statements made to the U.S. government.[7] According to some reports, U.S. companies provide

---

[3] Potomac Institute Cyber Center, *Weak Links in Communications Supply Chain Threatens Us All* (2012) (potomacinstitute.org/attachments/article/1276/Cyber%20paper%20Barnett.pdf).

[4] House Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Cong. (Oct. 8, 2012).

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

[6] Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC 18-42, ¶ 13 (Rel. Apr. 18, 2018).

[7] U.S. Department of Commerce, *Secretary Ross Announces Activation of ZTE Denial Order in Response To Repeated False Statements to the U.S. Government* (Apr. 16, 2018) (press

more than a quarter of the components in ZTE equipment and mobile devices.[8] ZTE has appealed the ban,[9] and announced that it has "halted majoring operating activities."[10] The President has also recently stated his intent to grant some relief to ZTE.

C. The National Defense Authorization Act (NDAA)

The FY2018 NDAA included language prohibiting the U.S. government from purchasing hardware, software, or services from Kaspersky Lab, which is a Russian firm. The language was included due to suspicions that Kaspersky Lab's technology could serve as espionage tools for the Russian government.[11] The current draft of the FY2019 NDAA includes a provision prohibiting government agencies from procuring or obtaining, or contracting with an entity that uses, telecommunications equipment or services "as a substantial or essential component of any system, or as a critical technology as part of any system" produced by certain entities, including Huawei and ZTE.[12] Agencies would be required to submit a report within 180 days after enactment of the bill to implement the prohibition, including explanations by each agency of their planned response measures to ensure compliance under the prohibition, where the manufacturer of a component in the supply chain is not readily known.[13]

III. WITNESSES

Dr. Charles Clancy
Director and Professor
Hume Center for National Security and Technology
Virginia Polytechnic Institute

Mr. Clete Johnson
Partner
Wilkinson Barker Knauer, LLP

Ms. Samm Sacks
Senior Fellow, Technology Policy Program
Center for Strategic and International Studies

---

release). This is the second major BIS action against ZTE in the past two years. In March 2017, ZTE agreed to pay $1.19 billion to settle allegations that it had illegally shipped equipment to Iran and North Korea and then mislead the U.S. government about it. ZTE has appealed the ban.

[8] *US Companies Banned from Selling Components to ZTE*, TechCrunch (Apr. 16, 2018).

[9] *ZTE Asks US Commerce Department to Suspend Business Ban*, Reuters (May 6, 2018).

[10] *China's ZTE Ceases Major Operations After US Trade Ban*, Bloomberg (May 9, 2018).

[11] *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, § 1634(a)-(b) (2017).

[12] H.R. 5515, sec. 866.

[13] *Id*.