II

115TH CONGRESS
2D SESSION

S. 2391

To prohibit the United States Government from using or contracting with an entity that uses certain telecommunications services or equipment, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 7, 2018

Mr. COTTON (for himself, Mr. CORNYN, and Mr. RUBIO) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To prohibit the United States Government from using or contracting with an entity that uses certain telecommunications services or equipment, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ‘‘Defending U.S. Government Communications Act’’.

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) In its 2011 ‘‘Annual Report to Congress on Military and Security Developments Involving the

People's Republic of China'', the Department of Defense stated, ''China's defense industry has benefited from integration with a rapidly expanding civilian economy and science and technology sector, particularly elements that have access to foreign technology. Progress within individual defense sectors appears linked to the relative integration of each, through China's civilian economy, into the global production and R&D chain . . . Information technology companies in particular, including Huawei, Datang, and Zhongxing, maintain close ties to the PLA.''.

(2) In a 2011 report titled ''The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector'', the United States China Commission stated that ''[n]ational security concerns have accompanied the dramatic growth of China's telecom sector. . . . Additionally, large Chinese companies—particularly those 'national champions' prominent in China's 'going out' strategy of overseas expansion—are directly subject to direction by the Chinese Communist Party, to include support for PRC state policies and goals.''.

(3) The Commission further stated in its report that ''[f]rom this point of view, the clear economic

benefits of foreign investment in the U.S. must be weighed against the potential security concerns related to infrastructure components coming under the control of foreign entities. This seems particularly applicable in the telecommunications industry, as Chinese companies continue systematically to acquire significant holdings in prominent global and U.S. telecommunications and information technology companies.''.

(4) In its 2011 Annual Report to Congress, the United States China Commission stated that ``[t]he extent of the state's control of the Chinese economy is difficult to quantify . . . There is also a category of companies that, though claiming to be private, are subject to state influence. Such companies are often in new markets with no established SOE leaders and enjoy favorable government policies that support their development while posing obstacles to foreign competition. Examples include Chinese telecoms giant Huawei and such automotive companies as battery maker BYD and vehicle manufacturers Geely and Chery.''.

(5) General Michael Hayden, who served as Director of the Central Intelligence Agency and Director of the National Security Agency, stated in July

2013 that Huawei had ''shared with the Chinese state intimate and extensive knowledge of foreign telecommunications systems it is involved with''.

(6) The Federal Bureau of Investigation, in a February 2015 Counterintelligence Strategy Partnership Intelligence Note stated that, ''[w]ith the expanded use of Huawei Technologies Inc. equipment and services in U.S. telecommunications service provider networks, the Chinese Government's potential access to U.S. business communications is dramatically increasing. Chinese Government-supported telecommunications equipment on U.S. networks may be exploited through Chinese cyber activity, with China's intelligence services operating as an advanced persistent threat to U.S. networks.''.

(7) The FBI further stated in its February 2015 counterintelligence note that ''China makes no secret that its cyber warfare strategy is predicated on controlling global communications network infrastructure''.

(8) At a hearing before the Committee on Armed Services of the House of Representatives on September 30, 2015, Deputy Secretary of Defense Robert Work, responding to a question about the use of Huawei telecommunications equipment, stat-

ed, "In the Office of the Secretary of Defense, absolutely not. And I know of no other—I don't believe we operate in the Pentagon, any [Huawei] systems in the Pentagon.".

(9) At that hearing, the Commander of the United States Cyber Command, Admiral Mike Rogers, responding to a question about why such Huawei telecommunications equipment is not used, stated, "As we look at supply chain and we look at potential vulnerabilities within the system, that it is a risk we felt was unacceptable.".

(10) In March 2017, ZTE Corporation pled guilty to conspiring to violate the International Emergency Economic Powers Act by illegally shipping U.S.-origin items to Iran, paying the United States Government a penalty of $892,360,064 for activity between January 2010 and January 2016.

(11) The Department of the Treasury's Office of Foreign Assets Control issued a subpoena to Huawei as part of a Federal investigation of alleged violations of trade restrictions on Cuba, Iran, Sudan, and Syria.

(12) In the bipartisan "Investigative Report on the United States National Security Issues Posed by Chinese Telecommunication Companies Huawei and

ZTE'' released in 2012 by the Permanent Select Committee on Intelligence of the House of Representatives, it was recommended that ''U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts. Similarly, government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment in their systems.''.

SEC. 3. PROHIBITION ON CERTAIN TELECOMMUNICATIONS SERVICES OR EQUIPMENT.

(a) PROHIBITION ON AGENCY USE OR PROCUREMENT.—The head of an agency may not procure or obtain, may not extend or renew a contract to procure or obtain, and may not enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(b) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5, United States Code.

(2) COVERED FOREIGN COUNTRY.—The term "covered foreign country" means the People's Republic of China.

(3) COVERED TELECOMMUNICATIONS EQUIPMENT OR SERVICES.—The term "covered telecommunications equipment or services" means any of the following:

(A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(B) Telecommunications services provided by such entities or using such equipment.

(C) Telecommunications equipment or services produced or provided by an entity that the head of the relevant agency reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

○