

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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Defending U.S. Gov-  
5 ernment Communications Act”.

6 **SEC. 2. FINDINGS.**

7 Congress makes the following findings:

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

1 People’s Republic of China”, the Department of De-  
2 fense stated, “China’s defense industry has benefited  
3 from integration with a rapidly expanding civilian  
4 economy and science and technology sector, particu-  
5 larly elements that have access to foreign technology.  
6 Progress within individual defense sectors appears  
7 linked to the relative integration of each, through  
8 China’s civilian economy, into the global production  
9 and R&D chain . . . Information technology compa-  
10 nies in particular, including Huawei, Datang, and  
11 Zhongxing, maintain close ties to the PLA.”

12 (2) In a 2011 report titled “The National Secu-  
13 rity Implications of Investments and Products from  
14 the People’s Republic of China in the Telecommuni-  
15 cations Sector”, the United States China Commis-  
16 sion stated that “[n]ational security concerns have  
17 accompanied the dramatic growth of China’s telecom  
18 sector. . . . Additionally, large Chinese companies—  
19 particularly those ‘national champions’ prominent in  
20 China’s ‘going out’ strategy of overseas expansion—  
21 are directly subject to direction by the Chinese Com-  
22 munist Party, to include support for PRC state poli-  
23 cies and goals.”

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

1 benefits of foreign investment in the U.S. must be  
2 weighed against the potential security concerns re-  
3 lated to infrastructure components coming under the  
4 control of foreign entities. This seems particularly  
5 applicable in the telecommunications industry, as  
6 Chinese companies continue systematically to ac-  
7 quire significant holdings in prominent global and  
8 U.S. telecommunications and information technology  
9 companies.”.

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

23 (5) General Michael Hayden, who served as Di-  
24 rector of the Central Intelligence Agency and Direc-  
25 tor of the National Security Agency, stated in July

1 2013 that Huawei had “shared with the Chinese  
2 state intimate and extensive knowledge of foreign  
3 telecommunications systems it is involved with”.

4 (6) The Federal Bureau of Investigation, in a  
5 February 2015 Counterintelligence Strategy Part-  
6 nership Intelligence Note stated that, “[w]ith the ex-  
7 panded use of Huawei Technologies Inc. equipment  
8 and services in U.S. telecommunications service pro-  
9 vider networks, the Chinese Government’s potential  
10 access to U.S. business communications is dramati-  
11 cally increasing. Chinese Government-supported tele-  
12 communications equipment on U.S. networks may be  
13 exploited through Chinese cyber activity, with Chi-  
14 na’s intelligence services operating as an advanced  
15 persistent threat to U.S. networks.”.

16 (7) The FBI further stated in its February  
17 2015 counterintelligence note that “China makes no  
18 secret that its cyber warfare strategy is predicated  
19 on controlling global communications network infra-  
20 structure”.

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

1 ed, “In the Office of the Secretary of Defense, abso-  
2 lutely not. And I know of no other—I don’t believe  
3 we operate in the Pentagon, any [Huawei] systems  
4 in the Pentagon.”.

5 (9) At that hearing, the Commander of the  
6 United States Cyber Command, Admiral Mike Rog-  
7 ers, responding to a question about why such  
8 Huawei telecommunications equipment is not used,  
9 stated, “As we look at supply chain and we look at  
10 potential vulnerabilities within the system, that it is  
11 a risk we felt was unacceptable.”.

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

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

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

1 ZTE” released in 2012 by the Permanent Select  
2 Committee on Intelligence of the House of Rep-  
3 resentatives, it was recommended that “U.S. govern-  
4 ment systems, particularly sensitive systems, should  
5 not include Huawei or ZTE equipment, including in  
6 component parts. Similarly, government contrac-  
7 tors—particularly those working on contracts for  
8 sensitive U.S. programs—should exclude ZTE or  
9 Huawei equipment in their systems.”.

10 **SEC. 3. PROHIBITION ON CERTAIN TELECOMMUNICATIONS**

11 **SERVICES OR EQUIPMENT.**

12 (a) PROHIBITION ON AGENCY USE OR PROCURE-  
13 MENT.—The head of an agency may not procure or obtain,  
14 may not extend or renew a contract to procure or obtain,  
15 and may not enter into a contract (or extend or renew  
16 a contract) with an entity that uses any equipment, sys-  
17 tem, or service that uses covered telecommunications  
18 equipment or services as a substantial or essential compo-  
19 nent of any system, or as critical technology as part of  
20 any system.

21 (b) DEFINITIONS.—In this section:

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

1           (2) COVERED FOREIGN COUNTRY.—The term  
2 “covered foreign country” means the People’s Re-  
3 public of China.

4           (3) COVERED TELECOMMUNICATIONS EQUIP-  
5 MENT OR SERVICES.—The term “covered tele-  
6 communications equipment or services” means any  
7 of the following:

8           (A) Telecommunications equipment pro-  
9 duced by Huawei Technologies Company or  
10 ZTE Corporation (or any subsidiary or affiliate  
11 of such entities).

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

14           (C) Telecommunications equipment or  
15 services produced or provided by an entity that  
16 the head of the relevant agency reasonably be-  
17 lieves to be an entity owned or controlled by, or  
18 otherwise connected to, the government of a  
19 covered foreign country.

○