

115TH CONGRESS
2D SESSION

H. R. 4747

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

IN THE HOUSE OF REPRESENTATIVES

JANUARY 9, 2018

Mr. CONAWAY (for himself and Ms. CHENEY) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

A BILL

To prohibit the 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 The Congress finds the following:

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 that, “China’s defense industry has ben-
3 efitated from integration with a rapidly expanding ci-
4 vilian economy and science and technology sector,
5 particularly elements that have access to foreign
6 technology. Progress within individual defense sec-
7 tors appears linked to the relative integration of
8 each, through China’s civilian economy, into the
9 global production and R&D chain . . . Information
10 technology companies in particular, including
11 Huawei, Datang, and Zhongxing, maintain close ties
12 to the PLA.”.

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

1 (3) The Commission further stated in its report
2 that “[f]rom this point of view, the clear economic
3 benefits of foreign investment in the U.S. must be
4 weighed against the potential security concerns re-
5 lated to infrastructure components coming under the
6 control of foreign entities. This seems particularly
7 applicable in the telecommunications industry, as
8 Chinese companies continue systematically to ac-
9 quire significant holdings in prominent global and
10 U.S. telecommunications and information technology
11 companies.”.

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

1 (5) General Michael Hayden, who served as Di-
2 rector of the Central Intelligence Agency and Direc-
3 tor of the National Security Agency, stated in July
4 2013 that Huawei had “shared with the Chinese
5 state intimate and extensive knowledge of foreign
6 telecommunications systems it is involved with.”.

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

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

24 (8) At a hearing before the Committee on
25 Armed Services of the House of Representatives on

1 September 30, 2015, Deputy Secretary of Defense
2 Robert Work, responding to a question about the
3 use of Huawei telecommunications equipment, stat-
4 ed, “In the Office of the Secretary of Defense, abso-
5 lutely not. And I know of no other—I don’t believe
6 we operate in the Pentagon, any [Huawei] systems
7 in the Pentagon.”.

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

15 (10) In March 2017, ZTE Corporation pled
16 guilty to conspiring to violate the International
17 Emergency Economic Powers Act by illegally ship-
18 ping U.S.-origin items to Iran, paying the United
19 States Government a penalty of \$892,360,064 dol-
20 lars for activity between January 2010 and January
21 2016.

22 (11) The Treasury Department’s Office of For-
23 eign Assets Control issued a subpoena to Huawei as
24 part of a Federal investigation of alleged violations

1 of trade restrictions on Cuba, Iran, Sudan, and
2 Syria.

3 (12) In the bipartisan House Permanent Select
4 Committee on Intelligence “Investigative Report on
5 the United States National Security Issues Posed by
6 Chinese Telecommunication Companies Huawei and
7 ZTE” released in 2012, it was recommended that
8 “U.S. government systems, particularly sensitive
9 systems, should not include Huawei or ZTE equip-
10 ment, including in component parts. Similarly, gov-
11 ernment contractors – particularly those working on
12 contracts for sensitive U.S. programs – should ex-
13 clude ZTE or Huawei equipment in their systems.”.

14 **SEC. 3. PROHIBITION ON CERTAIN TELECOMMUNICATIONS**
15 **SERVICES OR EQUIPMENT.**

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

25 (b) DEFINITIONS.—In this section:

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

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

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

11 (A) Telecommunications equipment pro-
12 duced by Huawei Technologies Company or
13 ZTE Corporation (or any subsidiary or affiliate
14 of such entities).

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

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

○