

113TH CONGRESS
2D SESSION

H. R. 4505

To direct the Comptroller General of the United States and the Chief Information Officer of the Department of Defense to assess the cloud security requirements of the Department of Defense.

IN THE HOUSE OF REPRESENTATIVES

APRIL 28, 2014

Ms. TSONGAS (for herself, Mr. KILMER, Mr. LARSEN of Washington, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Armed Services, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To direct the Comptroller General of the United States and the Chief Information Officer of the Department of Defense to assess the cloud security requirements of the Department of Defense.

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 “DOD Cloud Security
5 Act”.

1 **SEC. 2. ASSESSMENT OF DEPARTMENT OF DEFENSE CLOUD**
2 **SECURITY REQUIREMENTS.**

3 (a) COMPTROLLER GENERAL RESPONSIBILITIES.—

4 The Comptroller General of the United States shall—

5 (1) review and summarize the best practices re-
6 lating to cloud security by reviewing the practices of
7 other Federal departments and agencies and com-
8 mercial cloud providers;

9 (2) assess the cloud capacity of the Department
10 of Defense and such other departments and agencies
11 by assessing how and to what extent the Department
12 has adopted commercial cloud; and

13 (3) assess the opportunities for the Department
14 to utilize cloud computing in lieu of or in addition
15 to conventional computing.

16 (b) CHIEF INFORMATION OFFICER RESPONSIBIL-
17 ITIES.—The Chief Information Officer of the Department
18 of Defense shall—

19 (1) determine the security requirements that
20 are necessary for any cloud service to store Depart-
21 ment of Defense information, including—

22 (A) by individually detailing security re-
23 quirements for each Department of Defense im-
24 pact level and security classification level; and

25 (B) by providing a justification to the
26 Committees on Armed Services of the Senate

1 and House of Representatives for any discrep-
2 ancy between security requirements for dif-
3 ferent provider types;

4 (2) conduct a threat-based assessment of
5 whether security controls resident in commercial
6 cloud services and the cloud services of other Fed-
7 eral departments and agencies meet the security re-
8 quirements determined under paragraph (2), includ-
9 ing—

10 (A) by determining what services can and
11 cannot be provided by commercial cloud ven-
12 dors, based on such security requirements;

13 (B) by providing justification for why such
14 determinations were made by citing, as appro-
15 priate, industry responses to requests for infor-
16 mation and capability statement that confirm
17 the conclusions of the Department of Defense;
18 and

19 (C) by requesting that commercial vendors
20 submit their plans for how they can adapt their
21 systems to the unique and dynamic cyber de-
22 fense requirements of the Department of De-
23 fense;

24 (3) require any government-owned, operated, or
25 unique system that is or will be designed to provide

1 cloud capabilities for the Department of Defense to
2 be certified and accredited through the same proc-
3 ess, and to the same standards, that is used to cer-
4 tify and accredit commercial service providers; and

5 (4) ensure that, as part of any Department of
6 Defense pilot demonstrations with commercial cloud
7 vendors—

8 (A) an analysis is conducted of—

9 (i) requiring the Defense Information
10 Systems Agency to work with commercial
11 service providers to extend the Department
12 of Defense Information Network to com-
13 mercial service providers that are issued
14 provisional authority to operate for De-
15 partment of Defense impact levels 1 and 2
16 in order to leverage the commercial service
17 providers for secure connections to the De-
18 partment of Defense Information Network;

19 (ii) the benefits and challenges relat-
20 ing to how the secure connections would be
21 enabled and delivered as a service by the
22 DISA cloud broker to the commercial serv-
23 ice providers who have achieved provisional
24 authority to operate for Department of De-
25 fense impact levels 1 and 2;

1 (iii) requiring the Defense Informa-
2 tion Systems Agency to address the ability
3 of commercial service providers to provide
4 service for Department of Defense impact
5 levels 3 through 5 using logical separation;

6 (iv) the ability of commercial service
7 providers to provide innovative solutions to
8 the separation of customer data and sup-
9 porting resources that do not rely on phys-
10 ical separation;

11 (v) the benefits and challenges regard-
12 ing the consideration of such solutions for
13 equivalence to physical separation; and

14 (vi) the benefits and challenges of hy-
15 brid solutions for providing cloud services;
16 and

17 (B) the Chief Information Officer provides
18 to the Committees on Armed Services of the
19 Senate and House of Representatives a briefing
20 on the matters referred to in subparagraph (A)
21 by not later than 30 days after the conclusion
22 of such pilot demonstration.

○