.....

(Original Signature of Member)

113TH CONGRESS
2D SESSION

H. R. _____

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

Ms. TSONGAS introduced the following bill; which was referred to the Committee on _____

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.

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 ''DOD Cloud Security Act''.

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

(a) COMPTROLLER GENERAL RESPONSIBILITIES.—The Comptroller General of the United States shall—

(1) review and summarize the best practices relating to cloud security by reviewing the practices of other Federal departments and agencies and commercial cloud providers;

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

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

(b) CHIEF INFORMATION OFFICER RESPONSIBILITIES.—The Chief Information Officer of the Department of Defense shall—

(1) determine the security requirements that are necessary for any cloud service to store Department of Defense information, including—

(A) by individually detailing security requirements for each Department of Defense impact level and security classification level; and

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

and House of Representatives for any discrepancy between security requirements for different provider types;

(2) conduct a threat-based assessment of whether security controls resident in commercial cloud services and the cloud services of other Federal departments and agencies meet the security requirements determined under paragraph (2), including—

(A) by determining what services can and cannot be provided by commercial cloud vendors, based on such security requirements;

(B) by providing justification for why such determinations were made by citing, as appropriate, industry responses to requests for information and capability statement that confirm the conclusions of the Department of Defense; and

(C) by requesting that commercial vendors submit their plans for how they can adapt their systems to the unique and dynamic cyber defense requirements of the Department of Defense;

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

cloud capabilities for the Department of Defense to be certified and accredited through the same process, and to the same standards, that is used to certify and accredit commercial service providers; and

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

(A) an analysis is conducted of—

(i) requiring the Defense Information Systems Agency to work with commercial service providers to extend the Department of Defense Information Network to commercial service providers that are issued provisional authority to operate for Department of Defense impact levels 1 and 2 in order to leverage the commercial service providers for secure connections to the Department of Defense Information Network;

(ii) the benefits and challenges relating to how the secure connections would be enabled and delivered as a service by the DISA cloud broker to the commercial service providers who have achieved provisional authority to operate for Department of Defense impact levels 1 and 2; and

(iii) requiring the Defense Information Systems Agency to address the ability of commercial service providers to provide service for Department of Defense impact levels 3 through 5 using logical separation;

(iv) the ability of commercial service providers to provide innovative solutions to the separation of customer data and supporting resources that do not rely on physical separation;

(v) the benefits and challenges regarding the consideration of such solutions for equivalence to physical separation; and

(vi) the benefits and challenges of hybrid solutions for providing cloud services; and

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