114TH CONGRESS
2D SESSION

S. _____

To promote innovation and realize the efficiency gains and economic benefits of on-demand computing by accelerating the acquisition and deployment of innovative technology and computing resources throughout the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MORAN (for himself and Mr. UDALL) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To promote innovation and realize the efficiency gains and economic benefits of on-demand computing by accelerating the acquisition and deployment of innovative technology and computing resources throughout the Federal Government, 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This Act may be cited as the ''Modernizing Outdated and Vulnerable Equipment and Information Technology Act of 2016'' or the ''MOVE IT Act''.

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) National Institute of Standards and Technology Special Publication 800–145 describes cloud computing as an evolving paradigm for information technology that is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

(2) Together, the efficiencies, cost savings, and greater computing power enabled by cloud computing has the potential to—

(A) eliminate inappropriate duplication, reduce costs, and address waste, fraud, and abuse in providing Government services that are publicly available;

(B) address the critical need for cybersecurity by design; and

(C) move the Federal Government into a broad digital-services delivery model that could transform the fashion in which the Federal Government provides services to the people of the United States.

(b) PURPOSES.—The purposes of this Act are to—

(1) accelerate the acquisition and deployment of cloud computing services by addressing key impediments and roadblocks in funding, development, and acquisition practices;

(2) support and expand an efficient Federal certification standard for qualifying cloud services providers under the Federal Risk and Authorization Management Program using a ''qualify once, use many times'' efficiency model that strikes an appropriate balance between—

(A) encouraging the adoption of strong security practices to protect against the harm of cyber intrusions and hacks; and

(B) avoiding the imposition of unduly burdensome and restrictive requirements on cloud computing service providers that would deter investment in innovative cloud computing services;

(3) assist agencies in migrating to cloud computing services by providing guidance and oversight of agency enterprise-wide information technology portfolios suitable for and identifiable as suitable for a cloud-based delivery model; and

(4) provide for Federal agencies to procure cloud computing services that adhere to sound security practices.

SEC. 3. FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM.

(a) IN GENERAL.—Except as provided under subsection (b), a covered agency may not store or process Government information on a Federal information system with any cloud service provider, unless the provider has an authorization to operate, or a provisional authorization to operate, covering the proposed scope of work, from the covered agency or the Joint Authorization Board. A covered agency operating under a provisional authorization to operate shall issue an authorization to operate as soon as practicable and may not rely on the provisional authorization to operate for the duration of the scope of work.

(b) WAIVER OF REQUIREMENTS.—

(1) IN GENERAL.—The Director of National Intelligence, or a designee of the Director, may waive the applicability to any national security system of any provision of this section if the Director of National Intelligence, or the designee, determines that such waiver is in the interest of national security.

(2) NOTIFICATION.—Not later than 30 days after exercising a waiver under this subsection, the

Director of National Intelligence, or the designee of the Director, as the case may be, shall submit to the Committee on Homeland Security and Governmental Affairs and the Select Committee on Intelligence of the Senate and the Committee on Oversight and Government Reform and the Permanent Select Committee on Intelligence of the House of Representatives a statement describing and justifying the waiver.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as limiting the ability of the Office of Management and Budget to update or modify Federal guidelines relating to the security of cloud computing.

SEC. 4. EXPANDED INDUSTRY COLLABORATION AND METRICS DEVELOPMENT FOR THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM OFFICE.

(a) IN GENERAL.—The Director shall coordinate with the Federal Risk and Authorization Management Program Office to establish mandatory guidelines for the submission of an application for an authorization to operate and related materials to the Federal Risk and Authorization Management Program Office.

(b) CONTENTS.—The guidelines established under subsection (a) shall streamline and accelerate the Federal

Risk and Authorization Management Program accreditation process by meeting the following requirements:

(1) Not less frequently than monthly, report to the applicant the status, expected time to completion, and other key indicators related to compliance for an application for authorization to operate submitted to the Federal Risk and Authorization Management Program Office.

(2) Enhanced training and industry liaison opportunities for covered agencies and cloud service providers.

(3) A clarification of—

(A) the role and authority of third party assessment organization in the Federal Risk and Authorization Management Program process for authorizations to operate by covered agencies;

(B) the extent to which the Federal Risk and Authorization Management Program Office may identify and begin to accept or rely upon certifications from other standards development organizations or third party assessment organization; and

(C) the responsibility of covered agencies to sponsor a Federal Risk and Authorization

Management Program authorization to operate as part of making Federal Risk and Authorization Management Program compliance a condition for entering into a contract or providing cloud computing services to a covered agency.

(c) FEDRAMP LIAISON GROUP.—

(1) IN GENERAL.—The Director, in coordination with the Program Management Office and the National Institute of Standards and Technology, shall host a public-private industry cloud commercial working group (in this subsection referred to as the ''FedRAMP Liaison Group'') representing cloud service providers.

(2) COMPOSITION AND FUNCTIONS.—The FedRAMP Liaison Group—

(A) shall include representatives of cloud service providers;

(B) may include such working groups as are determined appropriate by the FedRAMP Liaison Group;

(C) shall be hosted by the General Services Administration, who shall convene plenary meetings on a quarterly basis with individual working groups meeting as frequently as determined by the group; and

(D) shall consult with and provide recommendations directly to the Program Management Office and the Joint Authorization Board of the Federal Risk and Authorization Management Program regarding the operations, processes improvements, and best practices of the Office and Board.

(3) FACA EXEMPTION.—The Federal Advisory Committee Act shall not apply to the FedRAMP Liaison Group.

(d) PROVIDING DEDICATED AGENCY SUPPORT.—The Program Management Office shall work with each covered agency to support and guide the efforts of the agency—

(1) to establish and issue the authorization to operate for the agency;

(2) to facilitate authorization approval, support, and direct interfacing with cloud service providers; and

(3) to facilitate partnership among agencies to efficiently support activities related to obtaining an authorization to operate.

(e) METRICS.—The Director, in coordination with the National Institute of Standards and Technology and the FedRAMP Liaison Group, shall establish key performance

metrics for the Federal Risk and Authorization Management Program Office, which shall include—

(1) recommendations for maximum time limits for the completion of authorizations to operate by service categories of cloud service providers, not to exceed six months;

(2) targets for the streamlining of the authorization to operate through the use of innovative templates and transparent submission requirements; and

(3) recommendations for satisfying Federal continuous monitoring requirements.

(f) REPORT REQUIRED.—Not later than one year after the date of the enactment of this Act, the Director shall submit to the Committees on Appropriations and Oversight and Government Reform of the House of Representatives and the Committees on Appropriations and Homeland Security and Governmental Affairs of the Senate a report on the effectiveness and efficiency of the Federal Risk and Authorization Management Program Office.

SEC. 5. ADDITIONAL BUDGET AUTHORITIES FOR THE MODERNIZATION OF IT SYSTEMS.

(a) ASSESSMENT OF CLOUD FIRST IMPLEMENTATION.—Not later than 90 days after the date of the enactment of this Act, the Director, in consultation with the Chief Information Officers Council, shall assess cloud

computing opportunities and issue policies and guidelines for the adoption of Governmentwide programs providing for a standardized approach to security assessment and operational authorization for cloud computing products and services.

(b) INFORMATION TECHNOLOGY SYSTEM MODERNIZATION AND WORKING CAPITAL FUND.—

(1) ESTABLISHMENT.—There is established in each covered agency an information technology system modernization and working capital fund (hereafter ''IT working capital fund'') for necessary expenses for the agency described in paragraph (2).

(2) SOURCE OF FUNDS.—Amounts may be deposited into an IT working capital fund as follows:

(A) Reprogramming of funds, including reprogramming of any funds available on the date of enactment of this Act for the operation and maintenance of legacy systems, in compliance with any applicable reprogramming law or guidelines of the Committees on Appropriations of the House of Representatives and the Senate.

(B) Transfer of funds, including transfer of any funds available on the date of enactment of this Act for the operation and maintenance

of legacy systems, but only if transfer authority is specifically provided for by law.

(C) Amounts made available through discretionary appropriations.

(3) USE OF FUNDS.—An IT working capital fund established under paragraph (1) may be used only for the following:

(A) The replacement of a legacy information technology system.

(B) The transition to cloud computing and innovative platforms and technologies subject to a transition plan for any project that costs more than $5,000,000 and approved by the Federal Chief Information Officer according to such guidelines as the Office of Management and Budget may designate.

(C) To assist and support agency efforts to provide adequate, risk-based, and cost-effective information technology capabilities that address evolving threats to information security.

(D) Developmental, modernization, and enhancement activities of information technology.

(4) EXISTING FUNDS.—An IT working capital fund may not be used to supplant funds provided for the operation and maintenance of any system al-

ready within an appropriation for the agency at the time of establishment of the IT working capital fund.

(5) REPROGRAMMING AND TRANSFER OF FUNDS.—The head of each covered agency shall prioritize funds within the IT working capital fund to be used initially for cost savings activities approved by the Federal Chief Information Officer, in consultation with the Chief Information Officer of the covered agency. The head of each covered agency may—

(A) reprogram any amounts saved as a direct result of such activities for deposit into the applicable IT working capital fund, consistent with paragraph (2)(A), except that any such reprogramming of amounts in excess of $500,000 shall be reported to the Committees on Appropriations of the House of Representatives and the Senate 30 days in advance of such reprogramming; and

(B) may transfer any amounts saved as a direct result of such activities for deposit into the applicable IT working capital fund, consistent with paragraph (2)(B), except that any such transfer of amounts in excess of $500,000

shall be reported to the Committees on Appropriations of the House of Representatives and the Senate 30 days in advance of such transfer.

(6) RETURN OF FUNDS.—Any funds deposited into an IT working capital fund must be obligated no later than 3 years after the date of such deposit. Any funds that are unobligated 3 years after such date shall be rescinded and deposited into the general fund of the Treasury and reported to the Committees on Appropriations of the House of Representatives and the Senate.

(7) SEMIANNUAL REPORT REQUIRED.—Not later than 6 months after the date of the enactment of this Act, and semiannually thereafter, the head of any covered agency that uses an IT working capital fund shall submit to the Committees on Appropriations and Oversight and Government Reform of the House of Representatives and the Committees on Appropriations and Homeland Security and Governmental Affairs of the Senate a report on the obligation and expenditure of funds made available under this section.

(c) GAO REPORT.—Not later than one year after the date of the enactment of this Act, and annually thereafter for five years, the Comptroller General of the United

States shall submit to the Committees on Appropriations and Oversight and Government Reform of the House of Representatives and the Committees on Appropriations and Homeland Security and Governmental Affairs of the Senate a report—

(1) on the implementation and operation of each IT working capital fund established under this section;

(2) that identifies current practices and compares the practices with industry best practices in areas such as the effective oversight and governance of a cloud computing working capital fund; and

(3) that describes the basis for the use and operation of an IT working capital fund, the efficacy of the working capital fund to accelerate technology transitions, and recommendations for further improvement for the working capital fund.

SEC. 6. DEFINITIONS.

In this Act:

(1) AUTHORIZATION TO OPERATE.—The term ''authorization to operate'' means an approval and accreditation, including a provisional authorization to operate, regarding the security and operational qualifications of a cloud computing service provider to offer secure, reliable cloud computing service to a

covered agency, that may be issued by the Joint Authorization Board, any successor entity, or the head of a covered agency.

(2) CLOUD COMPUTING.—The term ''cloud computing'' has the meaning given that term by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document thereto.

(3) CLOUD SERVICE PROVIDER.—The term ''cloud service provider'' means an entity offering cloud computing infrastructure, platforms, or software for commercial and Government entities.

(4) COVERED AGENCY.—The term ''covered agency'' means each agency listed in section 901(b) of title 31, United States Code.

(5) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(6) FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM OFFICE.—The term ''Federal Risk and Authorization Management Program Office'' or ''Program Management Office'' means the Federal Risk and Authorization Management Program Office, or any successor thereto.

(7) INFORMATION SYSTEM.—The term ''information system'' has the meaning given that term under section 3502 of title 44, United States Code.

(8) INFORMATION TECHNOLOGY.—The term ''information technology'' has the meaning given that term under section 11101 of title 40, United States Code.

(9) LEGACY INFORMATION TECHNOLOGY SYSTEM.—The term ''legacy information technology system'' means an outdated or obsolete information technology that is no longer supported by the originating vendor or manufacturer.

(10) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given that term under section 3552 of title 44, United States Code.

(11) THIRD PARTY ASSESSMENT ORGANIZATION.—The term ''third party assessment organization'' means a third party accreditation body that conducts a conformity assessment of a could service data provider to ensure the provider meets security and operational guidelines issued by the Federal Risk and Authorization Management Program Office.