

114TH CONGRESS
2D SESSION

S. 3263

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

JULY 14, 2016

Mr. MORAN (for himself, Mr. UDALL, Mr. DAINES, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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.

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4 This Act may be cited as the “Modernizing Outdated
5 and Vulnerable Equipment and Information Technology
6 Act of 2016” or the “MOVE IT Act”.

1 **SEC. 2. FINDINGS AND PURPOSES.**

2 (a) FINDINGS.—Congress finds the following:

3 (1) National Institute of Standards and Tech-
4 nology Special Publication 800–145 describes cloud
5 computing as an evolving paradigm for information
6 technology that is a model for enabling ubiquitous,
7 convenient, on-demand network access to a shared
8 pool of configurable computing resources (i.e., net-
9 works, servers, storage, applications, and services)
10 that can be rapidly provisioned and released with
11 minimal management effort or service provider inter-
12 action.

13 (2) Together, the efficiencies, cost savings, and
14 greater computing power enabled by cloud com-
15 puting has the potential to—

16 (A) eliminate inappropriate duplication, re-
17 duce costs, and address waste, fraud, and abuse
18 in providing Government services that are pub-
19 licly available;

20 (B) address the critical need for cybersecu-
21 rity by design; and

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

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

2 (1) accelerate the acquisition and deployment of
3 cloud computing services by addressing key impedi-
4 ments and roadblocks in funding, development, and
5 acquisition practices;

6 (2) support and expand an efficient Federal
7 certification standard for qualifying cloud services
8 providers under the Federal Risk and Authorization
9 Management Program using a “qualify once, use
10 many times” efficiency model that strikes an appro-
11 priate balance between—

12 (A) encouraging the adoption of strong se-
13 curity practices to protect against the harm of
14 cyber intrusions and hacks; and

15 (B) avoiding the imposition of unduly bur-
16 densome and restrictive requirements on cloud
17 computing service providers that would deter
18 investment in innovative cloud computing serv-
19 ices;

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

1 (4) provide for Federal agencies to procure
2 cloud computing services that adhere to sound secu-
3 rity practices.

4 **SEC. 3. FEDERAL RISK AND AUTHORIZATION MANAGEMENT**
5 **PROGRAM.**

6 (a) IN GENERAL.—Except as provided under sub-
7 section (b), a covered agency may not store or process
8 Government information on a Federal information system
9 with any cloud service provider, unless the provider has
10 an authorization to operate, or a provisional authorization
11 to operate, covering the proposed scope of work, from the
12 covered agency or the Joint Authorization Board. A cov-
13 ered agency operating under a provisional authorization
14 to operate shall issue an authorization to operate as soon
15 as practicable and may not rely on the provisional author-
16 ization to operate for the duration of the scope of work.

17 (b) WAIVER OF REQUIREMENTS.—

18 (1) IN GENERAL.—The Director of National In-
19 telligence, or a designee of the Director, may waive
20 the applicability to any national security system of
21 any provision of this section if the Director of Na-
22 tional Intelligence, or the designee, determines that
23 such waiver is in the interest of national security.

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

1 Director of National Intelligence, or the designee of
2 the Director, as the case may be, shall submit to the
3 Committee on Homeland Security and Governmental
4 Affairs and the Select Committee on Intelligence of
5 the Senate and the Committee on Oversight and
6 Government Reform and the Permanent Select Com-
7 mittee on Intelligence of the House of Representa-
8 tives a statement describing and justifying the waiv-
9 er.

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

14 **SEC. 4. EXPANDED INDUSTRY COLLABORATION AND**
15 **METRICS DEVELOPMENT FOR THE FEDERAL**
16 **RISK AND AUTHORIZATION MANAGEMENT**
17 **PROGRAM OFFICE.**

18 (a) IN GENERAL.—The Director shall coordinate
19 with the Federal Risk and Authorization Management
20 Program Office to establish mandatory guidelines for the
21 submission of an application for an authorization to oper-
22 ate and related materials to the Federal Risk and Author-
23 ization Management Program Office.

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

1 Risk and Authorization Management Program accredita-
2 tion process by meeting the following requirements:

3 (1) Not less frequently than monthly, report to
4 the applicant the status, expected time to comple-
5 tion, and other key indicators related to compliance
6 for an application for authorization to operate sub-
7 mitted to the Federal Risk and Authorization Man-
8 agement Program Office.

9 (2) Enhanced training and industry liaison op-
10 portunities for covered agencies and cloud service
11 providers.

12 (3) A clarification of—

13 (A) the role and authority of third party
14 assessment organization in the Federal Risk
15 and Authorization Management Program proc-
16 ess for authorizations to operate by covered
17 agencies;

18 (B) the extent to which the Federal Risk
19 and Authorization Management Program Office
20 may identify and begin to accept or rely upon
21 certifications from other standards development
22 organizations or third party assessment organi-
23 zation; and

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

1 Management Program authorization to operate
2 as part of making Federal Risk and Authoriza-
3 tion Management Program compliance a condi-
4 tion for entering into a contract or providing
5 cloud computing services to a covered agency.

6 (c) FEDRAMP LIAISON GROUP.—

7 (1) IN GENERAL.—The Director, in coordina-
8 tion with the Program Management Office and the
9 National Institute of Standards and Technology,
10 shall host a public-private industry cloud commercial
11 working group (in this subsection referred to as the
12 “FedRAMP Liaison Group”) representing cloud
13 service providers.

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

16 (A) shall include representatives of cloud
17 service providers;

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

21 (C) shall be hosted by the General Services
22 Administration, who shall convene plenary
23 meetings on a quarterly basis with individual
24 working groups meeting as frequently as deter-
25 mined by the group; and

1 (D) shall consult with and provide rec-
2 ommendations directly to the Program Manage-
3 ment Office and the Joint Authorization Board
4 of the Federal Risk and Authorization Manage-
5 ment Program regarding the operations, proc-
6 esses improvements, and best practices of the
7 Office and Board.

8 (3) FACA EXEMPTION.—The Federal Advisory
9 Committee Act shall not apply to the FedRAMP Li-
10 aison Group.

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

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

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

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

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

1 metrics for the Federal Risk and Authorization Manage-
2 ment Program Office, which shall include—

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

7 (2) targets for the streamlining of the author-
8 ization to operate through the use of innovative tem-
9 plates and transparent submission requirements; and

10 (3) recommendations for satisfying Federal con-
11 tinuous monitoring requirements.

12 (f) REPORT REQUIRED.—Not later than one year
13 after the date of the enactment of this Act, the Director
14 shall submit to the Committees on Appropriations and
15 Oversight and Government Reform of the House of Rep-
16 resentatives and the Committees on Appropriations and
17 Homeland Security and Governmental Affairs of the Sen-
18 ate a report on the effectiveness and efficiency of the Fed-
19 eral Risk and Authorization Management Program Office.

20 **SEC. 5. ADDITIONAL BUDGET AUTHORITIES FOR THE MOD-**
21 **ERNIZATION OF IT SYSTEMS.**

22 (a) ASSESSMENT OF CLOUD FIRST IMPLEMENTA-
23 TION.—Not later than 90 days after the date of the enact-
24 ment of this Act, the Director, in consultation with the
25 Chief Information Officers Council, shall assess cloud

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

6 (b) INFORMATION TECHNOLOGY SYSTEM MOD-
7 ERNIZATION AND WORKING CAPITAL FUND.—

8 (1) ESTABLISHMENT.—There is established in
9 each covered agency an information technology sys-
10 tem modernization and working capital fund (here-
11 after “IT working capital fund”) for necessary ex-
12 penses for the agency described in paragraph (2).

13 (2) SOURCE OF FUNDS.—Amounts may be de-
14 posited into an IT working capital fund as follows:

15 (A) Reprogramming of funds, including re-
16 programming of any funds available on the date
17 of enactment of this Act for the operation and
18 maintenance of legacy systems, in compliance
19 with any applicable reprogramming law or
20 guidelines of the Committees on Appropriations
21 of the House of Representatives and the Sen-
22 ate.

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

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

3 (C) Amounts made available through dis-
4 cretionary appropriations.

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

8 (A) The replacement of a legacy informa-
9 tion technology system.

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

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

21 (D) Developmental, modernization, and en-
22 hancement activities of information technology.

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

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

4 (5) REPROGRAMMING AND TRANSFER OF
5 FUNDS.—The head of each covered agency shall
6 prioritize funds within the IT working capital fund
7 to be used initially for cost savings activities ap-
8 proved by the Federal Chief Information Officer, in
9 consultation with the Chief Information Officer of
10 the covered agency. The head of each covered agency
11 may—

12 (A) reprogram any amounts saved as a di-
13 rect result of such activities for deposit into the
14 applicable IT working capital fund, consistent
15 with paragraph (2)(A), except that any such re-
16 programming of amounts in excess of \$500,000
17 shall be reported to the Committees on Appro-
18 priations of the House of Representatives and
19 the Senate 30 days in advance of such re-
20 programming; and

21 (B) may transfer any amounts saved as a
22 direct result of such activities for deposit into
23 the applicable IT working capital fund, con-
24 sistent with paragraph (2)(B), except that any
25 such transfer of amounts in excess of \$500,000

1 shall be reported to the Committees on Appro-
2 priations of the House of Representatives and
3 the Senate 30 days in advance of such transfer.

4 (6) RETURN OF FUNDS.—Any funds deposited
5 into an IT working capital fund must be obligated
6 no later than 3 years after the date of such deposit.
7 Any funds that are unobligated 3 years after such
8 date shall be rescinded and deposited into the gen-
9 eral fund of the Treasury and reported to the Com-
10 mittees on Appropriations of the House of Rep-
11 resentatives and the Senate.

12 (7) SEMIANNUAL REPORT REQUIRED.—Not
13 later than 6 months after the date of the enactment
14 of this Act, and semiannually thereafter, the head of
15 any covered agency that uses an IT working capital
16 fund shall submit to the Committees on Appropria-
17 tions and Oversight and Government Reform of the
18 House of Representatives and the Committees on
19 Appropriations and Homeland Security and Govern-
20 mental Affairs of the Senate a report on the obliga-
21 tion and expenditure of funds made available under
22 this section.

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

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

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

9 (2) that identifies current practices and com-
 10 pares the practices with industry best practices in
 11 areas such as the effective oversight and governance
 12 of a cloud computing working capital fund; and

13 (3) that describes the basis for the use and op-
 14 eration of an IT working capital fund, the efficacy
 15 of the working capital fund to accelerate technology
 16 transitions, and recommendations for further im-
 17 provement for the working capital fund.

18 **SEC. 6. DEFINITIONS.**

19 In this Act:

20 (1) **AUTHORIZATION TO OPERATE.**—The term
 21 “authorization to operate” means an approval and
 22 accreditation, including a provisional authorization
 23 to operate, regarding the security and operational
 24 qualifications of a cloud computing service provider
 25 to offer secure, reliable cloud computing service to a

1 covered agency, that may be issued by the Joint Au-
2 thorization Board, any successor entity, or the head
3 of a covered agency.

4 (2) CLOUD COMPUTING.—The term “cloud
5 computing” has the meaning given that term by the
6 National Institute of Standards and Technology in
7 NIST Special Publication 800–145 and any amend-
8 atory or superseding document thereto.

9 (3) CLOUD SERVICE PROVIDER.—The term
10 “cloud service provider” means an entity offering
11 cloud computing infrastructure, platforms, or soft-
12 ware for commercial and Government entities.

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

16 (5) DIRECTOR.—The term “Director” means
17 the Director of the Office of Management and Budg-
18 et.

19 (6) FEDERAL RISK AND AUTHORIZATION MAN-
20 AGEMENT PROGRAM OFFICE.—The term “Federal
21 Risk and Authorization Management Program Of-
22 fice” or “Program Management Office” means the
23 Federal Risk and Authorization Management Pro-
24 gram Office, or any successor thereto.

1 (7) INFORMATION SYSTEM.—The term “infor-
2 mation system” has the meaning given that term
3 under section 3502 of title 44, United States Code.

4 (8) INFORMATION TECHNOLOGY.—The term
5 “information technology” has the meaning given
6 that term under section 11101 of title 40, United
7 States Code.

8 (9) LEGACY INFORMATION TECHNOLOGY SYS-
9 TEM.—The term “legacy information technology sys-
10 tem” means an outdated or obsolete information
11 technology that is no longer supported by the origi-
12 nating vendor or manufacturer.

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

17 (11) THIRD PARTY ASSESSMENT ORGANIZA-
18 TION.—The term “third party assessment organiza-
19 tion” means a third party accreditation body that
20 conducts a conformity assessment of a cloud service
21 data provider to ensure the provider meets security
22 and operational guidelines issued by the Federal
23 Risk and Authorization Management Program Of-
24 fice.

