

.....  
(Original Signature of Member)

114TH CONGRESS  
2D SESSION

**H. R.**

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 HOUSE OF REPRESENTATIVES

Mr. HURD of Texas (for himself, Ms. KELLY of Illinois, Mrs. COMSTOCK, Mr. CONNOLLY, Mr. KILMER, and Mr. LIEU of California) introduced the following bill; which was 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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Modernizing Outdated  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

5 **SEC. 2. FINDINGS AND PURPOSES.**

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

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

17 (2) Together, the efficiencies, cost savings, and  
18 greater computing power enabled by cloud com-  
19 puting has the potential to—

20 (A) eliminate inappropriate duplication, re-  
21 duce costs, and address waste, fraud, and abuse  
22 in providing Government services that are pub-  
23 licly available;

24 (B) address the critical need for cybersecu-  
25 rity by design; and

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

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

7           (1) accelerate the acquisition and deployment of  
8           cloud computing services by addressing key impedi-  
9           ments and roadblocks in funding, development, and  
10          acquisition practices;

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

17                  (A) encouraging the adoption of strong se-  
18                  curity practices to protect against the harm of  
19                  cyber intrusions and hacks; and

20                  (B) avoiding the imposition of undue bur-  
21                  densome and restrictive requirements on cloud  
22                  computing service providers that would deter  
23                  investment in innovative cloud computing serv-  
24                  ices;

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

6           (4) provide for Federal agencies to procure  
7           cloud computing services that adhere to sound secu-  
8           rity practices.

9   **SEC. 3. FEDERAL RISK AND AUTHORIZATION MANAGEMENT**  
10                           **PROGRAM.**

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

22           (b) **WAIVER OF REQUIREMENTS.**—

23           (1) **IN GENERAL.**—The Director of National In-  
24           telligence, or a designee of the Director, may waive  
25           the applicability to any national security system of

1 any provision of this section if the Director of Na-  
2 tional Intelligence, or the designee, determines that  
3 such waiver is in the interest of national security.

4 (2) NOTIFICATION.—Not later than 30 days  
5 after exercising a waiver under this subsection, the  
6 Director of National Intelligence, or the designee of  
7 the Director, as the case may be, shall submit to the  
8 Committee on Homeland Security and Governmental  
9 Affairs and the Select Committee on Intelligence of  
10 the Senate and the Committee on Oversight and  
11 Government Reform and the Permanent Select Com-  
12 mittee on Intelligence of the House of Representa-  
13 tives a statement describing and justifying the waiv-  
14 er.

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

19 **SEC. 4. EXPANDED INDUSTRY COLLABORATION AND**  
20 **METRICS DEVELOPMENT FOR THE FEDERAL**  
21 **RISK AND AUTHORIZATION MANAGEMENT**  
22 **PROGRAM OFFICE.**

23 (a) IN GENERAL.—The Director shall coordinate  
24 with the Federal Risk and Authorization Management  
25 Program Office to establish mandatory guidelines for the

1 submission of an application for an authorization to oper-  
2 ate and related materials to the Federal Risk and Author-  
3 ization Management Program Office.

4 (b) CONTENTS.—The guidelines established under  
5 subsection (a) shall streamline and accelerate the Federal  
6 Risk and Authorization Management Program accredita-  
7 tion process by meeting the following requirements:

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

14 (2) Enhanced training and industry liaison op-  
15 portunities for covered agencies and cloud service  
16 providers.

17 (3) A clarification of—

18 (A) the role and authority of third party  
19 assessment organization in the Federal Risk  
20 and Authorization Management Program proc-  
21 ess for authorizations to operate by covered  
22 agencies;

23 (B) the extent to which the Federal Risk  
24 and Authorization Management Program Office  
25 may identify and begin to accept or rely upon

1           certifications from other standards development  
2           organizations or third party assessment organi-  
3           zation; and

4           (C) the responsibility of covered agencies  
5           to sponsor a Federal Risk and Authorization  
6           Management Program authorization to operate  
7           as part of making Federal Risk and Authoriza-  
8           tion Management Program compliance a condi-  
9           tion for entering into a contract or providing  
10          cloud computing services to a covered agency.

11       (c) FEDRAMP LIAISON GROUP.—

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

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

21           (A) shall include representatives of cloud  
22          service providers;

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

1 (C) shall be hosted by the General Services  
2 Administration, who shall convene plenary  
3 meetings on a quarterly basis with individual  
4 working groups meeting as frequently as deter-  
5 mined by the group; and

6 (D) shall consult with and provide rec-  
7 ommendations directly to the Program Manage-  
8 ment Office and the Joint Authorization Board  
9 of the Federal Risk and Authorization Manage-  
10 ment Program regarding the operations, proc-  
11 esses improvements, and best practices of the  
12 Office and Board.

13 (3) FACA EXEMPTION.—The Federal Advisory  
14 Committee Act shall not apply to the FedRAMP Li-  
15 aison Group.

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

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

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

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

4           (e) METRICS.—The Director, in coordination with the  
5           National Institute of Standards and Technology and the  
6           FedRAMP Liaison Group, shall establish key performance  
7           metrics for the Federal Risk and Authorization Manage-  
8           ment Program Office, which shall include—

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

13          (2) targets for the streamlining of the author-  
14          ization to operate through the use of innovative tem-  
15          plates and transparent submission requirements; and

16          (3) recommendations for satisfying Federal con-  
17          tinuous monitoring requirements.

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

1 **SEC. 5. ADDITIONAL BUDGET AUTHORITIES FOR THE MOD-**  
2 **ERNIZATION OF IT SYSTEMS.**

3 (a) ASSESSMENT OF CLOUD FIRST IMPLEMENTA-  
4 TION.—Not later than 90 days after the date of the enact-  
5 ment of this Act, the Director, in consultation with the  
6 Chief Information Officers Council, shall assess cloud  
7 computing opportunities and issue policies and guidelines  
8 for the adoption of Governmentwide programs providing  
9 for a standardized approach to security assessment and  
10 operational authorization for cloud computing products  
11 and services.

12 (b) INFORMATION TECHNOLOGY SYSTEM MOD-  
13 ERNIZATION AND WORKING CAPITAL FUND.—

14 (1) ESTABLISHMENT.—There is established in  
15 each covered agency an information technology sys-  
16 tem modernization and working capital fund (here-  
17 after “IT working capital fund”) for necessary ex-  
18 penses for the agency described in paragraph (2).

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

21 (A) Reprogramming of funds, including re-  
22 programming of any funds available on the date  
23 of enactment of this Act for the operation and  
24 maintenance of legacy systems, in compliance  
25 with any applicable reprogramming law or  
26 guidelines of the Committees on Appropriations

1 of the House of Representatives and the Sen-  
2 ate.

3 (B) Transfer of funds, including transfer  
4 of any funds available on the date of enactment  
5 of this Act for the operation and maintenance  
6 of legacy systems, but only if transfer authority  
7 is specifically provided for by law.

8 (C) Amounts made available through dis-  
9 cretionary appropriations.

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

13 (A) The replacement of a legacy informa-  
14 tion technology system.

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

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

1 (D) Developmental, modernization, and en-  
2 hancement activities of information technology.

3 (4) EXISTING FUNDS.—An IT working capital  
4 fund may not be used to supplant funds provided for  
5 the operation and maintenance of any system al-  
6 ready within an appropriation for the agency at the  
7 time of establishment of the IT working capital  
8 fund.

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

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

1 (B) may transfer any amounts saved as a  
2 direct result of such activities for deposit into  
3 the applicable IT working capital fund, con-  
4 sistent with paragraph (2)(B), except that any  
5 such transfer of amounts in excess of \$500,000  
6 shall be reported to the Committees on Appro-  
7 priations of the House of Representatives and  
8 the Senate 30 days in advance of such transfer.

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

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

1       tion and expenditure of funds made available under  
2       this section.

3       (c) GAO REPORT.—Not later than one year after the  
4       date of the enactment of this Act, and annually thereafter  
5       for five years, the Comptroller General of the United  
6       States shall submit to the Committees on Appropriations  
7       and Oversight and Government Reform of the House of  
8       Representatives and the Committees on Appropriations  
9       and Homeland Security and Governmental Affairs of the  
10      Senate a report—

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

14           (2) that identifies current practices and com-  
15           pares the practices with industry best practices in  
16           areas such as the effective oversight and governance  
17           of a cloud computing working capital fund; and

18           (3) that describes the basis for the use and op-  
19           eration of an IT working capital fund, the efficacy  
20           of the working capital fund to accelerate technology  
21           transitions, and recommendations for further im-  
22           provement for the working capital fund.

23      **SEC. 6. DEFINITIONS.**

24      In this Act:

1           (1) AUTHORIZATION TO OPERATE.—The term  
2           “authorization to operate” means an approval and  
3           accreditation, including a provisional authorization  
4           to operate, regarding the security and operational  
5           qualifications of a cloud computing service provider  
6           to offer secure, reliable cloud computing service to a  
7           covered agency, that may be issued by the Joint Au-  
8           thorization Board, any successor entity, or the head  
9           of a covered agency.

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

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

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

22          (5) DIRECTOR.—The term “Director” means  
23          the Director of the Office of Management and Budg-  
24          et.

1           (6) FEDERAL RISK AND AUTHORIZATION MAN-  
2           AGEMENT PROGRAM OFFICE.—The term “Federal  
3           Risk and Authorization Management Program Of-  
4           fice” or “Program Management Office” means the  
5           Federal Risk and Authorization Management Pro-  
6           gram Office, or any successor thereto.

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

10          (8) INFORMATION TECHNOLOGY.—The term  
11          “information technology” has the meaning given  
12          that term under section 11101 of title 40, United  
13          States Code.

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

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

23          (11) THIRD PARTY ASSESSMENT ORGANIZA-  
24          TION.—The term “third party assessment organiza-  
25          tion” means a third party accreditation body that

1       conducts a conformity assessment of a cloud service  
2       data provider to ensure the provider meets security  
3       and operational guidelines issued by the Federal  
4       Risk and Authorization Management Program Of-  
5       fice.