

# **MOVE IT Act of 2016**

## ***Section by Section Summary***

**SECTION 1. SHORT TITLE.** The Modernizing Outdated and Vulnerable Equipment and Information Technology Act of 2016 or the MOVE IT Act.

### **SEC. 2. FINDINGS AND PURPOSES.**

Describes cloud computing and the bill's purpose to accelerate adoption of cloud computing by federal agencies.

### **SEC. 3. FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM.**

Prohibits federal agencies from storing or processing government information on a Federal IT system with a cloud service provider (CSP) unless the CSP has an authorization to operate (ATO). An ATO is an accreditation that the CSP meets federal guidelines for cybersecurity and continuous monitoring included in existing Federal Risk and Authorization Management Program (FedRAMP) and National Institute of Standards and Technology (NIST) guidance. DOD and DNI can issue waivers.

### **SEC. 4. EXPANDED INDUSTRY COLLABORATION AND METRICS DEVELOPMENT FOR THE FEDRAMP PROGRAM OFFICE.**

Requires OMB and GSA to work together to streamline and accelerate the FedRAMP accreditation process for CSPs that seek to provide services to federal agencies. Establishes a public-private liaison group ("FedRAMP Liaison Group") to facilitate information sharing and identify best practices for CSPs and the FedRAMP office. Directs GSA to support and guide agencies' efforts to issue ATOs to CSPs. Requires OMB and NIST to establish

performance metrics for the FedRAMP process of authorizing CSPs to sell cloud services to federal agencies. Requires OMB to submit a report to Congress on the effectiveness and efficiency of the FedRAMP office.

## **SEC. 5. ADDITIONAL BUDGET AUTHORITIES FOR TRANSITION TO CLOUD COMPUTING SERVICES.**

Requires agency chief information officers (CIOs) to assess cloud computing opportunities and issue policies and guidelines for the adoption of Government-wide programs providing for a standardized approach to security assessment and operational authorization for cloud computing products and services.

Establishes within each covered agency an information technology system modernization and working capital fund "IT working capital fund." The IT working capital fund may be funded through 1) reprogramming of funds intended for the operation and maintenance of legacy systems; 2) transfers of funds where specifically provided for by existing law; 3) cost savings realized on IT projects; or 4) discretionary appropriations.

The IT working capital funds can be used only for 1) facilitating the replacement of legacy IT systems; 2) transitioning to cloud computing services; 3) addressing information security threats; or 4) developmental, modernization, and enhancement activities.

The IT working capital fund may not be used to supplant funds provided for the operation and maintenance of existing IT systems. Agencies shall prioritize initial use of the fund for cost savings initiatives approved by the Federal CIO.

Authorizes agencies to reprogram funds for deposit within the IT working capital fund. Reprogramming amounts of \$500,000 or more shall be reported to the House and Senate Committees on Appropriations 30 days in advance. Funds within the IT working capital fund must be obligated within

three years. Unobligated funds return to the general fund of the Treasury after three years.

Agencies must report semiannually on use of the funds to the House Committees on Appropriations and Oversight and Government Reform and the Committees on Appropriations and Homeland Security and Governmental Affairs of the Senate. GAO must report one year after enactment on the implementation, operation and effectiveness of each IT working capital fund.

## **SEC. 6. DEFINITIONS.**

Defines terms used in the bill, including covered federal agencies affected by the bill's provisions.