.....

(Original Signature of Member)

115TH CONGRESS
1ST SESSION

H. R. _____

To enhance the innovation, security, and availability of Federal Government cloud services by establishing the Federal Risk and Authorization Management Program within the Office of Management and Budget Office of Electronic Government and by establishing a risk management, authorization, and continuous monitoring process to enable the Federal Government to leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Reform Act of 2014 and cloud-based operations, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. CONNOLLY introduced the following bill; which was referred to the Committee on _____

A BILL

To enhance the innovation, security, and availability of Federal Government cloud services by establishing the Federal Risk and Authorization Management Program within the Office of Management and Budget Office of Electronic Government and by establishing a risk management, authorization, and continuous monitoring process to enable the Federal Government to leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Reform Act of 2014 and cloud-based operations, 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 ''Federal Risk and Authorization Management Program Reform Act of 2018'' or the ''FedRAMP Authorization Act''.

SEC. 2. CODIFICATION OF THE FEDRAMP PROGRAM.

(a) AMENDMENT.—Chapter 36 of title 44, United States Code, is amended by adding at the end the following new sections:

''§ 3607. Federal Risk and Authorization Management Program

''(a) ESTABLISHMENT.—There is established within the General Services Administration, an office to be known as the FedRAMP Program Management Office that shall be responsible for the Federal Risk and Authorization Management Program. FedRAMP is a specific Government certification program that examines and accredits cloud service providers that offer Federal cloud computing services for sale, lease, or purchase to Federal agency cloud customers. The FedRAMP Program Management Office embodies the goal of a 'qualify once, use many times' process through the issuance of certifications in the form of provisional authorizations to operate.

''(b) COMPONENTS OF FEDRAMP.—There are established as components of FedRAMP the Joint Authorization Board and the Program Management Office, or such successor offices as the Office of Management and Budget, through the Office of Electronic Government may determine.

''(c) FEDRAMP DUTIES.—The Director of the Office of Management and Budget and the Administrator of General Services, or their designees, shall work together to do the following:

''(1) Issue guidance on categories and characteristics of information technology goods or services that are within the jurisdiction of FedRAMP and that require FedRAMP certification.

''(2) Issue guidance for the establishment and implementation of FedRAMP to conduct security assessments, reviews, and appropriate oversight of continuous monitoring of cloud services used by agencies.

''(3) Not later than 180 days after the date of the enactment of this section, and annually thereafter, submit to Congress a report on the status and performance of the FedRAMP Program Management Office, including the status and disposition of waiver requests to FedRAMP submitted to the

FedRAMP Program Management Office by agencies and a description of and progress towards meeting the metrics adopted by the FedRAMP Program Management Office pursuant to section 3608(e), as submitted to the Administrator by that Office.

"§ 3608. Roles and responsibilities of the FedRAMP Program Management Office

''(a) IMPLEMENTATION.—Upon delegation from the Office of Electronic Government, the Administrator shall oversee the implementation of FedRAMP, including—

''(1) appointing a Program Director to oversee the FedRAMP Program Management Office;

''(2) hiring professional staff as may be necessary for the effective operation of the FedRAMP Program Management Office, and such other activities as are essential to properly perform critical functions; and

''(3) such other actions as the Administrator may determine necessary to carry out this section.

''(b) AUTHORITY AND DUTIES.—The FedRAMP Program Management Office shall have the following authority and duties:

''(1) Provide guidance to agencies, regarding compliance with requirements, guidelines, and stand-

ards developed by the National Institute of Standards and Technology.

''(2) Provide guidance to third party assessment organizations in using and applying the requirements, guidelines, and standards adopted by FedRAMP.

''(3) Provide guidance to agencies on appropriate use of and acquisition of FedRAMP approved services, including the role of cloud brokers and cloud service integrators.

''(4) In consultation with the Director and the Secretary of Homeland Security, issue guidance for agencies on monitoring and reporting on the usage and demand of cloud computing, use of automation, and use of commercial cloud services to the fullest extent practical.

''(5) In consultation with the Federal Chief Information Officer, oversee and issue guidelines regarding the qualifications, roles, and responsibilities of third party assessment organizations, in consultation with the National Institute of Standards and Technology.

''(6) Develop standards and templates, including a summary risk report template for third party assessment organizations that informs the security

assessment report to complement the existing authorization package artifacts and serve as an authorization decision-making tool.

''(7) Coordinate with stakeholders to provide guidance and recommendations to FedRAMP. Stakeholders to include—

''(A) agency cloud customers;

''(B) cloud service providers;

''(C) third party assessment organizations;

''(D) agency Offices of Inspector General; and

''(E) the Government Accountability Office.

''(8) Establish and maintain a public comment process for newly issued or revised guidance adopted by FedRAMP.

''(c) EVALUATION OF AUTOMATION PROCEDURES.—The FedRAMP Program Management Office shall assess and evaluate available automation procedures to accelerate the processing of FedRAMP applications.

''(d) METRICS FOR CERTIFICATION.—The FedRAMP Program Management Office shall adopt specific metrics regarding the time, cost, and quality of the assessments necessary for completion of a FedRAMP authorization process in a manner that can be consistently tracked over

time, which shall be done in conjunction with the periodic testing and evaluation process pursuant to subchapter II of chapter 35 in a manner that minimizes the agency reporting burden.

"§ 3609. Roles and responsibilities of the Joint Authorization Board

''(a) ESTABLISHMENT.—There is established the Joint Authorization Board which shall consist of the Chief Information Officers or their designees of the Department of Defense, the Department of Homeland Security, and the General Services Administration.

''(b) ISSUANCE OF PROVISIONAL AUTHORIZATIONS TO OPERATE.—The Joint Authorization Board shall have the authority to issue provisional authorizations to operate to cloud service providers that meet FedRAMP security guidelines set forth in the Common Security Control Baseline.

''(c) DUTIES.—The Joint Authorization Board shall—

''(1) review and validate cloud service provider and third party assessment organization security assessment packages;

''(2) in consultation with the FedRAMP Program Management Office, serve as a resource for best practices to accelerate the FedRAMP process;

''(3) obtain such professional staff as may be necessary for the effective operation of FedRAMP and such other activities as are essential to properly perform critical functions;

''(4) such other roles and responsibilities as the FedRAMP Program Management Office may assign, as agreed to by the FedRAMP Program Management Office and members of the Joint Authorization Board; and

''(5) appoint technical representatives responsible for FedRAMP activities within each Joint Authorization Board agency.

''§ 3610. Roles and responsibilities of third party assessment organizations

''(a) REQUIREMENTS FOR CERTIFICATION.—The FedRAMP Program Management Office, in consultation with the Joint Authorization Board, shall determine the requirements for certification of third party assessment organizations. Such requirements may include developing or requiring certification programs for individuals employed by the third party assessment organizations who lead FedRAMP assessment teams.

''(b) ASSESSMENT.—Accredited third party assessment organizations shall assess, validate, and attest to the

quality and compliance of security assessment materials provided by cloud service providers.

''(c) SUMMARY RISK REPORT.—Accredited third party assessment organizations shall develop a risk report that summarizes the security assessment report to complement the existing authorization package artifacts and serve as an authorization decision making tool.

"§ 3611. Roles and responsibilities of agencies

''(a) IN GENERAL.—In implementing and enforcing the requirements of FedRAMP, Federal agency cloud customers shall—

''(1) create policies to implement FedRAMP requirements;

''(2) issue agency-specific authorizations to operate for Federal cloud computing services in compliance with subchapter II of chapter 35;

''(3) be in compliance with any FedRAMP requirements, unless a waiver is issued by the Director;

''(4) provide data to the Director on how agencies are meeting metrics as defined by the FedRAMP Program Management Office pursuant to section 3614(b); and

''(5) if applicable, ensure that any contract is in compliance with FedRAMP requirements.

''(b) SUBMISSION OF POLICIES REQUIRED.—Not later than 6 months after the date of the enactment of this section, Federal agency cloud customers shall submit to the Director the policies created pursuant to subsection (a)(1) for review and approval.

''(c) SUBMISSION OF AUTHORIZATIONS TO OPERATE REQUIRED.—Upon issuance of an authorization to operate, the head of the relevant agency shall provide a copy of the authorization to operate letter to the FedRAMP Program Management Office and the cloud service provider to enable the FedRAMP Program Management Office to track and assess all forms of authorizations to operate on a Governmentwide basis.

''(d) PRESUMPTION OF ADEQUACY.—Any provisional authorization to operate issued by the Joint Authorization Board shall be considered to be presumptively adequate by agencies, subject to technical or programmatic rebuttal by an agency that disagrees with adequacy or sufficiency of the certification. This rebuttable presumption of adequacy shall not derogate, modify, or alter the responsibility of any agency to ensure compliance with the subchapter II of chapter 35 for any Federal cloud computing services that the agency deploys.

''(e) WAIVER OR EXCEPTION.—The Chief Information Officer of each agency may request a waiver or excep-

tion to specific FedRAMP requirements. Such request for waiver shall be in accordance with the determinations and finding issued under section 3612(2). The determination and findings shall be submitted to the FedRAMP Program Management Office and the Director, along with such supporting articles as may be required under guidelines issued by FedRAMP.

''(f) AGENCY REPORTS REQUIRED.—Not later than 90 days after the date of which any guidance is issued pursuant to section 3608(b)(4) from the FedRAMP Program Management Office, the head of each agency shall submit to the Director a report on cloud computing usage and the potential demand for cloud computing.

"§ 3612. Roles and Responsibilities of the Office of Management and Budget

''The Director shall have the following duties:

''(1) Highlight current guidance or issue new guidance to ensure that an agency does not operate a Federal Government cloud computing service using Government data without issuing an authorization to operate issued by the agency that meets the requirements of subchapter II of chapter 35 and FedRAMP.

''(2) Issue guidance and templates for agency determinations and findings for waivers to the re-

quirements of FedRAMP (any request by an agency for such a waiver must set forth unique agency-specific technical, operational, or managerial requirements necessary for agency operations).

''(3) Define alternatives and agency best practices for compliance with the Trusted Internet Connection for agencies connecting to a cloud service provider.

''(4) Grant waivers or exceptions to specific FedRAMP requirements as may be necessary by the submission of agency determinations and findings that meet the OMB guidelines for FedRAMP waivers pursuant to paragraph (2).

''(5) Ensure agencies are in compliance with any guidance or other requirements issued related to FedRAMP.

''§ 3613. Funding of FedRAMP

''The FedRAMP Program Management Office may, to the extent deemed appropriate by the Administrator and in consultation with the Director, use funds contained within the Acquisition Services Fund described under section 321 of title 40 or such other funds as may be available for the operations of FedRAMP.

"§ 3614. Reporting

''(a) IN GENERAL.—Not later than 18 months after the date of the enactment of this section, and annually thereafter, the Director shall submit to the Committee on Oversight and Government Reform of the House of Representatives and the Committee on Homeland Security and Government Affairs of the Senate a report that includes the following:

''(1) The status, efficiency, and effectiveness of FedRAMP during the preceding year in authorizing and recertifying secure cloud solutions for Federal agency cloud customers.

''(2) The length of time for Federal agency cloud customers to issue authorizations to operate during the preceding year.

''(3) Agency requests for FedRAMP waivers.

''(4) Progress during the preceding year in advancing automation techniques to securely automate FedRAMP processes and to accelerate reporting as described in this section.

''(5) Number of cloud computing systems in use at each agency and the number of cloud computing authorizations to operate.

''(b) GAO REPORT.—Not later than 2 years after the date of enactment of this section, and every three years thereafter, the Comptroller General shall submit to the

Oversight and Government Reform Committee of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate an assessment of FedRAMP, third party assessment organizations, and Federal agency cloud customers, including the following:

''(1) An evaluation of the impact and continuing need for specific cloud security controls.

''(2) A review of the adequacy of resources to run FedRAMP.

''(3) The development of reusability and the potential for the use and adoption of reciprocal standards, whether from Government or the private sector, as substitutes for specific security controls in use by the FedRAMP Project Management Office.

''§ 3615. Definitions

''(a) IN GENERAL.—Except as provided under paragraph (2), the definitions under sections 3502 and 3552 apply to sections 3607 through 3614.

''(b) ADDITIONAL DEFINITIONS.—In sections 3607 through 3614:

''(1) ADMINISTRATOR.—The term 'Administrator' means the Administrator of General Services.

''(2) CLOUD BROKER.—The term 'cloud broker' means an entity that manages the use, performance,

and delivery of cloud computing services and negotiates relationships between cloud service providers and cloud consumers.

''(3) CLOUD COMPUTING.—The term 'cloud computing' means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (as defined by the National Institute of Standards and Technology pursuant to the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), including NIST Special Publication 800–145) or any successor thereto.

''(4) CLOUD SERVICE INTEGRATOR.—The term 'cloud service integrator' means a systems or service integrator that specializes in cloud computing services.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means a third party entity offering cloud computing services to the Federal Government.

''(6) COMMON SECURITY CONTROL BASELINE.—The term 'common security control baseline' means the guidance issued pursuant to section 3607(c)(2).

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

''(8) FEDERAL AGENCY CLOUD CUSTOMER.—The term 'Federal agency cloud customer' means an agency using cloud computing services.

''(9) FEDERALLY CONTROLLED INFORMATION SYSTEM.—The term 'federally controlled information system' or 'Federal information system' means an information system used or operated by a Federal agency cloud customer as set forth and in compliance with the guidelines and requirements of section 3554 of title 40.

''(10) FEDERAL GOVERNMENT CLOUD COMPUTING SERVICES.—The term 'Federal Government cloud computing services' means a cloud computing service that is used or operated by a Federal agency cloud customer upon a federally controlled information system.

''(11) FEDRAMP.—The term 'FedRAMP' means the Federal Risk and Authorization Management Program established under section 3607(a).

''(12) FEDRAMP PROGRAM MANAGEMENT OFFICE.—The term 'FedRAMP Program Management Office' means the office that administers FedRAMP.

''(13) FEDRAMP SECURITY CONTROLS BASELINE.—The term 'FedRAMP security controls baseline' means those security controls that cloud service providers and agencies must, at a minimum, address to receive a provisional authorization to operate, as defined by the FedRAMP Program Management Office.

''(14) JOINT AUTHORIZATION BOARD.—The term 'Joint Authorization Board' means the Joint Authorization Board established under section 3609.

''(15) TECHNICAL REPRESENTATIVE.—The term 'technical representative' means an agency's technical representative to the Joint Authorization Board designated by the member agency of the Joint Authorization Board.

''(16) THIRD PARTY ASSESSMENT ORGANIZATION.—The term 'third party assessment organization' means a third-party organization accredited by the Program Director of the FedRAMP Program Management Office to undertake conformity assessments of cloud service providers.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 36 of title 44, United States Code, is amended by adding at the end the following new item