AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
116–391

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM AUTHORIZATION ACT OF 2019

FEBRUARY 5, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mrs. CAROLYN B. MALONEY of New York, , from the Committee on Oversight and Reform, submitted the following

R E P O R T

[To accompany H.R. 3941]

[Including cost estimate of the Congressional Budget Office]

The Committee on Oversight and Reform, to whom was referred the bill (H.R. 3941) to enhance the innovation, security, and availability of cloud computing services used in the Federal Government by establishing the Federal Risk and Authorization Management Program within the General Services Administration 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 Modernization Act of 2014 and cloud-based operations, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

99–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Risk and Authorization Management Program Authorization Act of 2019" 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 the Federal Risk and Authorization Management Program. The Administrator of General Services, in accordance with the guidelines established pursuant to section 3612, shall establish a governmentwide program that provides the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies.

"(b) COMPONENTS OF FEDRAMP.—The Joint Authorization Board and the FedRAMP Program Management Office are established as components of FedRAMP.

"§ 3608. FedRAMP Program Management Office

"(a) GSA DUTIES.—

"(1) ROLES AND RESPONSIBILITIES.—The Administrator of General Services shall—

"(A) determine the categories and characteristics of cloud computing information technology goods or services that are within the jurisdiction of FedRAMP and that require FedRAMP authorization from the Joint Authorization Board or the FedRAMP Program Management Office;

"(B) develop, coordinate, and implement a process for the FedRAMP Program Management Office, the Joint Authorization Board, and agencies to review security assessments of cloud computing services pursuant to subsections (b) and (c) of section 3611, and appropriate oversight of continuous monitoring of cloud computing services; and

"(C) ensure the continuous improvement of FedRAMP.

"(2) IMPLEMENTATION.—The Administrator shall oversee the implementation of FedRAMP, including—

"(A) appointing a Program Director to oversee the FedRAMP Program Management Office;

"(B) 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;

"(C) entering into interagency agreements to detail personnel on a reimbursable or non-reimbursable basis to assist the FedRAMP Program Management Office and the Joint Authorization Board in discharging the responsibilities of the Office under this section; and

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

"(b) DUTIES.—The FedRAMP Program Management Office shall have the following duties:

"(1) Provide guidance to independent assessment organizations, validate the independent assessments, and apply the requirements and guidelines adopted in section 3609(c)(5).

"(2) Oversee and issue guidelines regarding the qualifications, roles, and responsibilities of independent assessment organizations.

"(3) Develop templates and other materials to support the Joint Authorization Board and agencies in the authorization of cloud computing services to increase the speed, effectiveness, and transparency of the authorization process, consistent with standards defined by the National Institute of Standards and Technology.

"(4) Establish and maintain a public comment process for proposed guidance before the issuance of such guidance by FedRAMP.

"(5) Issue FedRAMP authorization for any authorizations to operate issued by an agency that meets the requirements and guidelines described in paragraph (1).

"(6) Establish frameworks for agencies to use authorization packages processed by the FedRAMP Program Management Office and Joint Authorization Board.

"(7) Coordinate with the Secretary of Defense and the Secretary of Homeland Security to establish a framework for continuous monitoring and reporting required of agencies pursuant to section 3553.

"(8) Establish a centralized and secure repository to collect and share necessary data, including security authorization packages, from the Joint Authorization Board and agencies to enable better sharing and reuse to such packages across agencies.

"(c) EVALUATION OF AUTOMATION PROCEDURES.—

"(1) IN GENERAL.—The FedRAMP Program Management Office shall assess and evaluate available automation capabilities and procedures to improve the efficiency and effectiveness of the issuance of provisional authorizations to operate issued by the Joint Authorization Board and FedRAMP authorizations, including continuous monitoring of cloud environments and among cloud environments.

"(2) MEANS FOR AUTOMATION.—Not later than 1 year after the date of the enactment of this section and updated annually thereafter, the FedRAMP Program Management Office shall establish a means for the automation of security assessments and reviews.

"(d) METRICS FOR AUTHORIZATION.—The FedRAMP Program Management Office shall establish annual metrics regarding the time and quality of the assessments necessary for completion of a FedRAMP authorization process in a manner that can be consistently tracked over time in conjunction with the periodic testing and evaluation process pursuant to section 3554 in a manner that minimizes the agency reporting burden.

"§ 3609. Joint Authorization Board

"(a) ESTABLISHMENT.—There is established the Joint Authorization Board which shall consist of cloud computing experts, appointed by the Director in consultation with the Administrator, from each of the following:

"(1) The Department of Defense.

"(2) The Department of Homeland Security.

"(3) The General Services Administration.

"(4) Such other agencies as determined by the Director, in consultation with the Administrator.

"(b) ISSUANCE OF PROVISIONAL AUTHORIZATIONS TO OPERATE.—The Joint Authorization Board shall conduct security assessments of cloud computing services and issue provisional authorizations to operate to cloud service providers that meet FedRAMP security guidelines set forth in section 3608(b)(1).

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

"(1) develop and make publicly available on a website, determined by the Administrator, criteria for prioritizing and selecting cloud computing services to be assessed by the Joint Authorization Board;

"(2) provide regular updates on the status of any cloud computing service during the assessment and authorization process of the Joint Authorization Board;

"(3) review and validate cloud computing services and independent assessment organization security packages or any documentation determined to be necessary by the Joint Authorization Board to evaluate the system security of a cloud computing service;

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

"(5) establish requirements and guidelines for security assessments of cloud computing services, consistent with standards defined by the National Institute of Standards and Technology, to be used by the Joint Authorization Board and agencies;

"(6) perform such other roles and responsibilities as the Administrator may assign, in consultation with the FedRAMP Program Management Office and members of the Joint Authorization Board; and

"(7) establish metrics and goals for reviews and activities associated with issuing provisional authorizations to operate and provide to the FedRAMP Program Management Office.

"(d) DETERMINATIONS OF DEMAND FOR CLOUD COMPUTING SERVICES.—The Joint Authorization Board shall consult with the Chief Information Officers Council established in section 3603 to establish a process for prioritizing and accepting the cloud

computing services to be granted a provisional authorization to operate through the Joint Authorization Board, which shall be made available on a public website.

"(e) DETAIL OF PERSONNEL.—To assist the Joint Authorization Board in discharging the responsibilities under this section, personnel of agencies may be detailed to the Joint Authorization Board for the performance of duties described under subsection (c).

"§ 3610. Independent assessment organizations

"(a) REQUIREMENTS FOR ACCREDITATION.—The Joint Authorization Board shall determine the requirements for certification of independent assessment organizations pursuant to section 3609. Such requirements may include developing or requiring certification programs for individuals employed by the independent assessment organizations who lead FedRAMP assessment teams.

"(b) ASSESSMENT.—Accredited independent assessment organizations may assess, validate, and attest to the quality and compliance of security assessment materials provided by cloud service providers.

"§ 3611. Roles and responsibilities of agencies

"(a) IN GENERAL.—In implementing the requirements of FedRAMP, the head of each agency shall, consistent with guidance issued by the Director pursuant to section 3612—

"(1) create policies to ensure cloud computing services used by the agency meet FedRAMP security requirements and other risk-based performance requirements as defined by the Director;

"(2) issue agency-specific authorizations to operate for cloud computing services in compliance with section 3554;

"(3) confirm whether there is a provisional authorization to operate in the cloud security repository established under section 3608(b)(10) issued by the Joint Authorization Board or a FedRAMP authorization issued by the FedRAMP Program Management Office before beginning an agency authorization for a cloud computing product or service;

"(4) to the extent practicable, for any cloud computing product or service the agency seeks to authorize that has received either a provisional authorization to operate by the Joint Authorization Board or a FedRAMP authorization by the FedRAMP Program Management Office, use the existing assessments of security controls and materials within the authorization package; and

"(5) provide data and information required to the Director pursuant to section 3612 to determine how agencies are meeting metrics as defined by the FedRAMP Program Management Office.

"(b) SUBMISSION OF POLICIES REQUIRED.—Not later than 6 months after the date of the enactment of this section, the head of each agency 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 or a provisional authorization to operate issued by an agency, the head of each agency shall provide a copy of the authorization to operate letter and any supplementary information required pursuant to section 3608(b) to the FedRAMP Program Management Office.

"(d) PRESUMPTION OF ADEQUACY.—

"(1) IN GENERAL.—The assessment of security controls and materials within the authorization package for provisional authorizations to operate issued by the Joint Authorization Board and agency authorizations to operate that receive FedRAMP authorization from the FedRAMP Program Management Office shall be presumed adequate for use in agency authorizations of cloud computing products and services.

"(2) INFORMATION SECURITY REQUIREMENTS.—The presumption under paragraph (1) does not modify or alter the responsibility of any agency to ensure compliance with subchapter II of chapter 35 for any cloud computing products or services used by the agency.

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

"The Director shall have the following duties:

"(1) Issue guidance to ensure that an agency does not operate a Federal Government cloud computing service using Government data without an authorization to operate issued by the agency that meets the requirements of subchapter II of chapter 35 and FedRAMP.

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

"(3) Review, analyze, and update guidance on the adoption, security, and use of cloud computing services used by agencies.

"(4) Ensure the Joint Authorization Board is in compliance with section 3609(c).

"(5) Adjudicate disagreements between the Joint Authorization Board and cloud service providers seeking a provisional authorization to operate through the Joint Authorization Board.

"(6) Promulgate regulations on the role of FedRAMP authorization in agency acquisition of cloud computing products and services that process unclassified information.

"§ 3613. Authorization of appropriations for FEDRAMP

"There is authorized to be appropriated $20,000,000 each year for the FedRAMP Program Management Office and the Joint Authorization Board.

"§ 3614. Reports to Congress

"Not later than 12 months after the date of the enactment of this section, and annually thereafter, the Director shall submit to the Committee on Oversight and Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following:

"(1) The status, efficiency, and effectiveness of FedRAMP Program Management Office and agencies during the preceding year in supporting the speed, effectiveness, sharing, reuse, and security of authorizations to operate for cloud computing products and services, including progress towards meeting the metrics adopted by the FedRAMP Program Management Office pursuant to section 3608(d) and the Joint Authorization Board pursuant to section 3609(c)(5).

"(2) Data on agency use of provisional authorizations to operate issued by the Joint Authorization Board and agency sponsored authorizations that receive FedRAMP authorization by the FedRAMP Program Management Office.

"(3) The length of time for the Joint Authorization Board to review applications for and issue provisional authorizations to operate.

"(4) The length of time for the FedRAMP Program Management Office to review agency applications for and issue FedRAMP authorization.

"(5) The number of provisional authorizations to operate issued by the Joint Authorization Board and FedRAMP authorizations issued by the FedRAMP Program Management Office for the previous year.

"(6) A review of progress made during the preceding year in advancing automation techniques to securely automate FedRAMP processes and to accelerate reporting as described in this section.

"(7) The number and characteristics of authorized cloud computing services in use at each agency consistent with guidance provided by the Director in section 3612.

"§ 3615. Federal Secure Cloud Advisory Committee

"(a) ESTABLISHMENT, PURPOSES, AND DUTIES.—

"(1) ESTABLISHMENT.—There is established a Federal Secure Cloud Advisory Committee (referred to in this section as the 'Committee') to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of cloud computing products and services to enable agency mission and administrative priorities.

"(2) PURPOSES.—The purposes of the Committee are the following:

"(A) To examine the operations of FedRAMP and determine ways that authorization processes can continuously be improved, including the following:

"(i) Measures to increase agency re-use of provisional authorizations to operate issued by the Joint Authorization Board.

"(ii) Proposed actions that can be adopted to reduce the cost of provisional authorizations to operate and FedRAMP authorizations for cloud service providers.

"(iii) Measures to increase the number of provisional authorizations to operate or FedRAMP authorizations for cloud computing services offered by small businesses (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

"(B) Collect information and feedback on agency compliance with and implementation of FedRAMP requirements.

"(C) Serve as a forum that facilitates communication and collaboration among the FedRAMP stakeholder community.

"(3) DUTIES.—The duties of the Committee are, at a minimum, the following:

"(A) Provide advice and recommendations to the Administrator, the Joint Authorization Board, and to agencies on technical, financial, programmatic, and operational matters regarding secure adoption of cloud computing services.

"(B) Submit reports as required.

"(b) MEMBERS.—

"(1) COMPOSITION.—The Committee shall be comprised of not more than 15 members who are qualified representatives from the public and private sectors, appointed by the Administrator, in consultation with the Administrator of the Office of Electronic Government, as follows:

"(A) The Administrator or the Administrator's designee, who shall be the Chair of the Committee.

"(B) At least 1 representative each from the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

"(C) At least 2 officials who serve as the Chief Information Security Officer within an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

"(D) At least 1 official serving as Chief Procurement Officer (or equivalent) in an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

"(E) At least 1 individual representing an independent assessment organization.

"(F) No fewer than 5 representatives from unique businesses that primarily provide cloud computing services or products, including at least 2 representatives from a small business (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a))).

"(G) At least 2 other government representatives as the Administrator determines to be necessary to provide sufficient balance, insights, or expertise to the Committee.

"(2) DEADLINE FOR APPOINTMENT.—Each member of the Committee shall be appointed not later than 30 days after the date of the enactment of this Act.

"(3) PERIOD OF APPOINTMENT; VACANCIES.—

"(A) IN GENERAL.—Each non-Federal member of the Committee shall be appointed for a term of 3 years, except that the initial terms for members may be staggered 1, 2, or 3 year terms to establish a rotation in which one-third of the members are selected each year. Any such member may be appointed for not more than 2 consecutive terms.

"(B) VACANCIES.—Any vacancy in the Committee shall not affect its powers, but shall be filled in the same manner in which the original appointment was made. Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

"(c) MEETINGS AND RULES OF PROCEDURES.—

"(1) MEETINGS.—The Committee shall hold not fewer than 3 meetings in a calendar year, at such time and place as determined by the Chair.

"(2) INITIAL MEETING.—Not later than 120 days after the date of the enactment of this section, the Committee shall meet and begin the operations of the Committee.

"(3) RULES OF PROCEDURE.—The Committee may establish rules for the conduct of the business of the Committee, if such rules are not inconsistent with this section or other applicable law.

"(d) EMPLOYEE STATUS.—

"(1) IN GENERAL.—A member of the Committee (other than a member who is appointed to the Committee in connection with another Federal appointment) shall not be considered an employee of the Federal Government by reason of any service as such a member, except for the purposes of section 5703 of title 5, relating to travel expenses.

"(2) PAY NOT PERMITTED.—A member of the Committee covered by paragraph (1) may not receive pay by reason of service on the panel.

"(e) APPLICABILITY TO THE FEDERAL ADVISORY COMMITTEE ACT.—Notwithstanding any other provision of law, the Federal Advisory Committee Act (5 U.S.C. App.) shall apply to the Committee, except that section 14 of such Act shall not apply.

"(f) HEARINGS AND EVIDENCE.—The Committee, or on the authority of the Committee, any subcommittee, may, for the purposes of carrying out this section, hold hearings, sit and act at such times and places, take testimony, receive evidence, and administer oaths.

"(g) CONTRACTING.—The Committee, may, to such extent and in such amounts as are provided in appropriation Acts, enter into contracts to enable the Committee to discharge its duties under this section.

"(h) INFORMATION FROM FEDERAL AGENCIES.—

"(1) IN GENERAL.—The Committee is authorized to secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government, information, suggestions, estimates, and statistics for the purposes of the Committee. Each department, bureau, agency, board, commission, office, independent establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Committee, upon request made by the Chair, the Chair of any subcommittee created by a majority of the Committee, or any member designated by a majority of the Committee.

"(2) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information may only be received, handled, stored, and disseminated by members of the Committee and its staff consistent with all applicable statutes, regulations, and Executive orders.

"(i) ASSISTANCE FROM AGENCIES.—

"(1) OTHER DEPARTMENTS AND AGENCIES.—In addition to the administration of the Committee by the General Services Administration, other agencies may provide to the Committee such services, funds, facilities, staff, and other support services as the head of the agency determines to be advisable and as is authorized by law.

"(2) DETAIL OF EMPLOYEES.—Any Federal Government employee may be detailed to the Committee without reimbursement from the Committee, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

"(j) POSTAL SERVICES.—The Committee may use the United States mails in the same manner and under the same conditions as agencies.

"(k) EXPERT AND CONSULTANT SERVICES.—The Committee is authorized to procure the services of experts and consultants in accordance with section 3109 of title 5, but at rates not to exceed the daily rate paid a person occupying a position at Level IV of the Executive Schedule under section 5315 of title 5.

"(l) REPORTS.—

"(1) INTERIM REPORTS.—The Committee may submit to the Administrator and Congress interim reports containing such findings, conclusions, and recommendations as have been agreed to by the Committee.

"(2) ANNUAL REPORTS.—Not later than 18 months after the date of the enactment of this section, and annually thereafter, the Committee shall submit to the Administrator and Congress a final report containing such findings, conclusions, and recommendations as have been agreed to by the Committee.

"§ 3616. Definitions

"(a) IN GENERAL.—Except as provided under subsection (b), the definitions under sections 3502 and 3552 apply to sections 3607 through this section.

"(b) ADDITIONAL DEFINITIONS.—In sections 3607 through this section:

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

"(2) AUTHORIZATION PACKAGE.—The term 'authorization package'—

"(A) means the essential information used to determine whether to authorize the operation of an information system or the use of a designated set of common controls; and

"(B) at a minimum, includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

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

"(4) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering cloud computing services to agencies.

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

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

"(7) FEDRAMP AUTHORIZATION.—The term 'FedRAMP authorization' means a cloud computing product or service that has received an agency authorization to operate and has been approved by the FedRAMP Program Management Office to meet requirements and guidelines established by the FedRAMP Program Management Office.

"(8) FEDRAMP PROGRAM MANAGEMENT OFFICE.—The term 'FedRAMP Program Management Office' means the office that administers FedRAMP established under section 3608.

"(9) INDEPENDENT ASSESSMENT ORGANIZATION.—The term 'independent 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.

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

(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 items:

"Sec.
"3607. Federal Risk and Authorization Management Program.
"3608. FedRAMP Program Management Office.
"3609. Joint Authorization Board.
"3610. Independent assessment organizations.
"3611. Roles and responsibilities of agencies.
"3612. Roles and responsibilities of the Office of Management and Budget.
"3613. Authorization of appropriations for FEDRAMP.
"3614. Reports to Congress.
"3615. Federal Secure Cloud Advisory Committee.
"3616. Definitions.".

(c) SUNSET.—This Act and any amendment made by this Act shall be repealed on the date that is 10 years after the date of the enactment of this Act.

(d) RULE OF CONSTRUCTION.—Nothing in this Act or any amendment made by this Act shall be construed as altering or impairing the authorities of the Director of the Office of Management and Budget or the Secretary of Homeland Security under subchapter II of chapter 35 of title 44, United States Code.

SUMMARY AND PURPOSE OF LEGISLATION

The Federal Risk and Authorization Management Program (FedRAMP) Authorization Act of 2019 would codify the FedRAMP Program at the General Services Administration (GSA). It would authorize GSA to establish a governmentwide program to provide a standardized approach to security assessment and authorization for cloud computing products and services.

BACKGROUND AND NEED FOR LEGISLATION

The Office of Management and Budget (OMB) established FedRAMP in December 2011 to provide joint authorizations and continuous security monitoring services for cloud services for all federal agencies.[1] According to the FedRAMP Program Management Office (PMO), the "primary objective is to provide a re-usable security authorization model by which Agencies can obtain safe, secure cloud service technologies to help modernize Federal IT [Information Technology]."[2]

A cloud service provider can take two different approaches to becoming FedRAMP certified: (1) seek a Provisional–Authority to Operate (P–ATO) from the Joint Authorization Board (JAB), an independent decision-making body for FedRAMP consisting of the Chief Information Officers from the Departments of Homeland Security and Defense and GSA; or (2) find an agency to sponsor the cloud service provider through the FedRAMP certification process with the FedRAMP PMO. Once an agency receives its FedRAMP certification, it is listed on the FedRAMP Marketplace, a central repository for agencies to find approved cloud services.

FedRAMP can be thought of as a method for thorough risk assessment and mitigation in the IT cloud arena. The federal govern-

[1] Office of Management and Budget, *Security Authorization and Information Systems in Cloud Computing Environments* (Dec. 8, 2011) (online at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fedrampmemo.pdf).

[2] Federal Risk and Authorization Management Program, *FedRAMP Accelerated: A Case Study for Change Within Government* (2017) (online at https://fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf).

ment regulates its risk in implementing cloud technology by determining the type of data that the system is storing such as Personal Identifiable Information or National Security data. FedRAMP sets security controls (i.e. multi-factor authentication or encryption requirements) based on standards established by the National Institute of Standards and Technology. FedRAMP standards have been commended for having "some of the best international standards for cloud security . . . [and] that provided customers with the confidence they needed to begin adopting the latest cloud technologies."[3]

The federal government spends roughly 80% of its $90 billion in IT spending on operations and maintenance of existing systems, including many legacy systems.[4] Programs like FedRAMP are critical to accelerating the government's adoption of modern and improved IT solutions. According to OMB, FedRAMP "has allowed agencies to adapt from arcane legacy technology to mission-centric and cost-effective cloud-based systems in a more rapid, consistent, and secure manner."[5]

The efficiencies and cost-savings gained from having a standardized authorization program benefits both agencies and the companies offering cloud services. Security authorizations can be onerous, but a FedRAMP certification enables both the government and the private sector to avoid duplicating security reviews, thus saving time, money, and effort. FedRAMP reports that if agencies reuse authorizations an average of six times, it equates to more than $250 million in cost avoidance.[6]

In 2015, the FedRAMP PMO requested feedback from government and industry stakeholders to help evaluate the program. They received both positive and negative feedback. For example, some stakeholders stated:

> [T]he JAB [Joint Authorization Board] authorization process took too long; the rigorous reviews did not always add value to a system's security; stakeholders were not clear on program expectations, which often seemed to be a moving target; and there was uncertainty about how to successfully complete the process in a defined timeframe. Venders felt that FedRAMP sometimes required a prohibitively high amount of resources and delayed or prevented them from doing business with the Federal Government. This was especially true for smaller vendors.[7]

While some cloud service providers continue to have similar complaints about FedRAMP, the program has made significant progress since its establishment to improve its processes, reduce the time to authorize cloud service offerings, and provide more transparency. New initiatives like FedRAMP Ready and FedRAMP

---

[3] *Id.*

[4] Government Accountability Office, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems* (June 2019) online at www.gao.gov/products/GAO-19-471).

[5] Office of the Federal Chief Information Officer, *Federal Cloud Computing Strategy—Cloud Smart* (June 2019) (online at https://cloud.cio.gov/strategy/#security).

[6] Federal Risk and Authorization Management Program, *About Us* (online at www.fedramp.gov/about/) (accessed January 22, 2020).

[7] Federal Risk and Authorization Management Program, *FedRAMP Accelerated: A Case Study for Change Within Government* (2017) (online at https://fedramp.gov/assets/resources/documents/FedRAMP_Accelerated_A_Case_Study_For_Change_Within_Government.pdf).

Accelerated are evidence of the program's agility and willingness to adapt.

For example, FedRAMP Accelerated, which was initiated in 2016, changed the time that a cloud service provider's capabilities would be surveyed to the beginning of the process rather than in the middle or end of the process. As a result, the JAB reduced the time it required to issue a P–ATO by 75% from an average of 12 to 24 months to only six months.[8]

By codifying the FedRAMP program at GSA, H.R. 3941 would continue this governmentwide and standardized approach to security assessment ad authorization for cloud computing products and services in order to help agencies modernize their information technology systems. The legislation would reduce duplication of security assessments and other obstacles to agency adoption of cloud products by establishing a "presumption of adequacy" for cloud technologies that have received FedRAMP certification. This presumption of adequacy means that the cloud service offering has met baseline security standards established by the program and should be considered approved for use across the federal government. The bill would also require GSA to work toward automating the FedRAMP process, which will lead to further standardization in security assessments and continuous monitoring of cloud services, increasing the efficiency for providers and agencies.

H.R. 3941 also requires FedRAMP to be more transparent. The bill requires the FedRAMP PMO and the JAB to develop and adopt metrics regarding the time and quality of security assessments used to issue FedRAMP authorizations. It also requires OMB to submit an annual report to Congress on the status, efficiency, and effectiveness of FedRAMP, including its progress towards meeting metrics consistently tracked over time and any progress made to automate FedRAMP processes.

The bill also establishes the Federal Secure Cloud Advisory Committee to ensure dialogue among GSA, agency cybersecurity and procurement officials, and industry for effective and ongoing coordination in acquisition and adoption of cloud products by the federal government. This committee will also provide a forum for industry to bring concerns to GSA and agencies in a public setting that fosters a collaborative problem-solving environment to continuously improve the program.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

The short title is the "Federal Risk and Authorization Management Program Authorization Act of 2019" or the "FedRAMP Authorization Act."

Section 2. Codification of the FedRAMP program

This section would establish the FedRAMP program within GSA and would establish as components of FedRAMP the JAB and the FedRAMP PMO. This section also would direct the Administrator of GSA to establish a governmentwide program to provide the au-

[8] Federal Risk and Authorization Management Program, *How FedRAMP Transformed JAB Authorizations to Take 75% Less Time* (Mar. 28, 2018) (online at www.fedramp.gov/how-fedramp-transformed-jab-authorizations-to-take-less-time/).

thoritative standardized approach to security assessment and authorization of cloud computing products and services that process unclassified information used by agencies.

To ensure effective operation of the FedRAMP program, this section also would assign roles and responsibilities in providing guidance and administering the program to GSA, the FedRAMP PMO, the JAB, independent assessment organizations, and OMB. The section also would require an annual report to Congress on the efficiency and effectiveness of the FedRAMP PMO and agencies in supporting the effectiveness and security of authorizations to operate for cloud computing products and services and other information such as the number of authorized cloud computing services in use at each agency. The bill would authorize to be appropriated $20 million for the FedRAMP program. Finally, this section would establish a Federal Secure Cloud Advisory Committee to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of cloud computing products and services to enable agency mission and administrative priorities.

LEGISLATIVE HISTORY

On July 24, 2019, Representative Gerald E. Connolly (D–VA) introduced H.R. 3941, the FedRAMP Authorization Act of 2019, which was referred to the Committee with Representative Mark Meadows (R–NC) as an original cosponsor.

COMMITTEE CONSIDERATION

On December 19, 2019, the Committee considered H.R. 3941 at a business meeting with a quorum present. Chairwoman Maloney offered an amendment in the nature of a substitute (ANS). The ANS was adopted by a voice vote, and the Committee ordered the bill reported favorably, as amended, by voice vote.

ROLL CALL VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following roll call votes occurred during the Committee's consideration of H.R. 3941:

No Roll Call Votes were taken on this bill.

EXPLANATION OF AMENDMENTS

During Committee consideration of the bill, Representative Carolyn Maloney (D–NY), Chairwoman of the Committee, offered an ANS that made certain technical changes to the bill. The Committee adopted the ANS by a voice vote.

LIST OF RELATED COMMITTEE HEARINGS

For the purposes of section 103(i) of H. Res. 6 of the 116th Congress, the following hearing was used to consider H.R. 3941: "To the Cloud! The Cloudy Role of FedRAMP in IT Modernization," held before the Subcommittee on Government Operations on July 17, 2019.

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee recommends the adoption of this bill (H.R. 3941) to authorize FedRAMP within GSA. In addition, the Committee affirms that further oversight findings and recommendations are reflected in the preceding section entitled Background and Need for Legislation.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

In accordance with clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee's performance goal or objective of this bill is to codify the Federal Risk and Authorization Management Program.

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

This bill does not relate to employment or access to public services and accommodations within the meaning of section 102(b)(3) of Public Law 104–1.

DUPLICATION OF FEDERAL PROGRAMS

In accordance with clause 3(c)(5) of rule XIII, no provision of this bill establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office (GAO) to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

DISCLOSURE OF DIRECTED RULE MAKINGS

This bill does not direct the completion of any specific rule makings within the meaning of section 551 of title 5, United States Code.

FEDERAL ADVISORY COMMITTEE ACT STATEMENT

The legislation establishes an advisory committee within the definition of Section 5(b) of the appendix to title 5, United States Code.

UNFUNDED MANDATES REFORM ACT STATEMENT

Pursuant to section 423 of the *Congressional Budget Act of 1974* the Committee has included a letter received from the Congressional Budget Office below.

EARMARK IDENTIFICATION

This bill does not include any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI of the House of Representatives.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(2)(B) of rule XIII of the Rules of the House of Representatives, the Committee includes below a cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the *Congressional Budget Act of 1974*.

NEW BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the House of Representatives, the cost estimate prepared by the Congressional Budget Office and submitted pursuant to section 402 of the *Congressional Budget Act of 1974* is as follows:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, February 3, 2020.

Hon. CAROLYN B. MALONEY,
Chairwoman, Committee on Oversight and Reform,
House of Representatives, Washington, DC.

DEAR MADAM CHAIRWOMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3941, the FedRAMP Authorization Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 3941, FedRAMP Authorization Act
As ordered reported by the House Committee on Oversight and Reform on December 19, 2019

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	100	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 3941 would establish a Federal Risk and Authorization Management Program within the General Services Administration. That program would establish a standardized approach throughout the government for acquiring and using security assessment and

cloud computing products and services. H.R. 3941 would authorize the appropriation of $20 million annually for this program.

The bill also would establish the Federal Secure Cloud Advisory Committee. Composed of 15 members, the committee would examine how the cloud process could be improved. Using information about the cost of other advisory committees, CBO estimates implementing this provision would cost about $3 million over the 2020–2025 period.

Assuming appropriation of the specified and estimated amounts, CBO estimates that in total, implementing H.R. 3941 would cost $100 million over the 2020–2025 period, primarily to carry out the Federal Risk and Authorization Management Program. The costs of the legislation (detailed in Table 1) fall within budget function 800 (general government).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 3941

	By fiscal year, millions of dollars—						
	2020	2021	2022	2023	2024	2025	2020–2025
Estimated Authorization	20	20	20	21	21	21	123
Estimated Outlays	*	17	20	21	21	21	100

* = between zero and $500,000.

The CBO staff contact for this estimate is Matthew Pickford. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

* * * * * * *

CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

Sec.
3601. Definitions.

* * * * * * *

3607. Federal Risk and Authorization Management Program.
3608. FedRAMP Program Management Office.
3609. Joint Authorization Board.
3610. Independent assessment organizations.
3611. Roles and responsibilities of agencies.
3612. Roles and responsibilities of the Office of Management and Budget.
3613. Authorization of appropriations for FEDRAMP.
3614. Reports to Congress.
3615. Federal Secure Cloud Advisory Committee.
3616. Definitions.

* * * * * * *

§ 3607. Federal Risk and Authorization Management Program

(a) ESTABLISHMENT.—There is established within the General Services Administration the Federal Risk and Authorization Management Program. The Administrator of General Services, in accordance with the guidelines established pursuant to section 3612, shall establish a governmentwide program that provides the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies.

(b) COMPONENTS OF FEDRAMP.—The Joint Authorization Board and the FedRAMP Program Management Office are established as components of FedRAMP.

§ 3608. FedRAMP Program Management Office

(a) GSA DUTIES.—

(1) ROLES AND RESPONSIBILITIES.—The Administrator of General Services shall—

(A) determine the categories and characteristics of cloud computing information technology goods or services that are within the jurisdiction of FedRAMP and that require FedRAMP authorization from the Joint Authorization Board or the FedRAMP Program Management Office;

(B) develop, coordinate, and implement a process for the FedRAMP Program Management Office, the Joint Authorization Board, and agencies to review security assessments of cloud computing services pursuant to subsections (b) and (c) of section 3611, and appropriate oversight of continuous monitoring of cloud computing services; and

(C) ensure the continuous improvement of FedRAMP.

(2) IMPLEMENTATION.—The Administrator shall oversee the implementation of FedRAMP, including—

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

(B) 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;

(C) entering into interagency agreements to detail personnel on a reimbursable or non-reimbursable basis to assist the FedRAMP Program Management Office and the Joint Authorization Board in discharging the responsibilities of the Office under this section; and

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

(b) DUTIES.—The FedRAMP Program Management Office shall have the following duties:

(1) Provide guidance to independent assessment organizations, validate the independent assessments, and apply the requirements and guidelines adopted in section 3609(c)(5).

(2) Oversee and issue guidelines regarding the qualifications, roles, and responsibilities of independent assessment organizations.

(3) Develop templates and other materials to support the Joint Authorization Board and agencies in the authorization of

cloud computing services to increase the speed, effectiveness, and transparency of the authorization process, consistent with standards defined by the National Institute of Standards and Technology.

(4) Establish and maintain a public comment process for proposed guidance before the issuance of such guidance by FedRAMP.

(5) Issue FedRAMP authorization for any authorizations to operate issued by an agency that meets the requirements and guidelines described in paragraph (1).

(6) Establish frameworks for agencies to use authorization packages processed by the FedRAMP Program Management Office and Joint Authorization Board.

(7) Coordinate with the Secretary of Defense and the Secretary of Homeland Security to establish a framework for continuous monitoring and reporting required of agencies pursuant to section 3553.

(8) Establish a centralized and secure repository to collect and share necessary data, including security authorization packages, from the Joint Authorization Board and agencies to enable better sharing and reuse to such packages across agencies.

(c) EVALUATION OF AUTOMATION PROCEDURES.—

(1) IN GENERAL.—The FedRAMP Program Management Office shall assess and evaluate available automation capabilities and procedures to improve the efficiency and effectiveness of the issuance of provisional authorizations to operate issued by the Joint Authorization Board and FedRAMP authorizations, including continuous monitoring of cloud environments and among cloud environments.

(2) MEANS FOR AUTOMATION.—Not later than 1 year after the date of the enactment of this section and updated annually thereafter, the FedRAMP Program Management Office shall establish a means for the automation of security assessments and reviews.

(d) METRICS FOR AUTHORIZATION.—The FedRAMP Program Management Office shall establish annual metrics regarding the time and quality of the assessments necessary for completion of a FedRAMP authorization process in a manner that can be consistently tracked over time in conjunction with the periodic testing and evaluation process pursuant to section 3554 in a manner that minimizes the agency reporting burden.

§ 3609. Joint Authorization Board

(a) ESTABLISHMENT.—There is established the Joint Authorization Board which shall consist of cloud computing experts, appointed by the Director in consultation with the Administrator, from each of the following:

(1) The Department of Defense.

(2) The Department of Homeland Security.

(3) The General Services Administration.

(4) Such other agencies as determined by the Director, in consultation with the Administrator.

(b) ISSUANCE OF PROVISIONAL AUTHORIZATIONS TO OPERATE.—The Joint Authorization Board shall conduct security assessments

of cloud computing services and issue provisional authorizations to operate to cloud service providers that meet FedRAMP security guidelines set forth in section 3608(b)(1).

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

(1) develop and make publicly available on a website, determined by the Administrator, criteria for prioritizing and selecting cloud computing services to be assessed by the Joint Authorization Board;

(2) provide regular updates on the status of any cloud computing service during the assessment and authorization process of the Joint Authorization Board;

(3) review and validate cloud computing services and independent assessment organization security packages or any documentation determined to be necessary by the Joint Authorization Board to evaluate the system security of a cloud computing service;

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

(5) establish requirements and guidelines for security assessments of cloud computing services, consistent with standards defined by the National Institute of Standards and Technology, to be used by the Joint Authorization Board and agencies;

(6) perform such other roles and responsibilities as the Administrator may assign, in consultation with the FedRAMP Program Management Office and members of the Joint Authorization Board; and

(7) establish metrics and goals for reviews and activities associated with issuing provisional authorizations to operate and provide to the FedRAMP Program Management Office.

(d) DETERMINATIONS OF DEMAND FOR CLOUD COMPUTING SERVICES.—The Joint Authorization Board shall consult with the Chief Information Officers Council established in section 3603 to establish a process for prioritizing and accepting the cloud computing services to be granted a provisional authorization to operate through the Joint Authorization Board, which shall be made available on a public website.

(e) DETAIL OF PERSONNEL.—To assist the Joint Authorization Board in discharging the responsibilities under this section, personnel of agencies may be detailed to the Joint Authorization Board for the performance of duties described under subsection (c).

§ 3610. Independent assessment organizations

(a) REQUIREMENTS FOR ACCREDITATION.—The Joint Authorization Board shall determine the requirements for certification of independent assessment organizations pursuant to section 3609. Such requirements may include developing or requiring certification programs for individuals employed by the independent assessment organizations who lead FedRAMP assessment teams.

(b) ASSESSMENT.—Accredited independent assessment organizations may assess, validate, and attest to the quality and compliance of security assessment materials provided by cloud service providers.

§ 3611. Roles and responsibilities of agencies

(a) IN GENERAL.—In implementing the requirements of FedRAMP, the head of each agency shall, consistent with guidance issued by the Director pursuant to section 3612—

(1) create policies to ensure cloud computing services used by the agency meet FedRAMP security requirements and other risk-based performance requirements as defined by the Director;

(2) issue agency-specific authorizations to operate for cloud computing services in compliance with section 3554;

(3) confirm whether there is a provisional authorization to operate in the cloud security repository established under section 3608(b)(10) issued by the Joint Authorization Board or a FedRAMP authorization issued by the FedRAMP Program Management Office before beginning an agency authorization for a cloud computing product or service;

(4) to the extent practicable, for any cloud computing product or service the agency seeks to authorize that has received either a provisional authorization to operate by the Joint Authorization Board or a FedRAMP authorization by the FedRAMP Program Management Office, use the existing assessments of security controls and materials within the authorization package; and

(5) provide data and information required to the Director pursuant to section 3612 to determine how agencies are meeting metrics as defined by the FedRAMP Program Management Office.

(b) SUBMISSION OF POLICIES REQUIRED.—Not later than 6 months after the date of the enactment of this section, the head of each agency 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 or a provisional authorization to operate issued by an agency, the head of each agency shall provide a copy of the authorization to operate letter and any supplementary information required pursuant to section 3608(b) to the FedRAMP Program Management Office.

(d) PRESUMPTION OF ADEQUACY.—

(1) IN GENERAL.—The assessment of security controls and materials within the authorization package for provisional authorizations to operate issued by the Joint Authorization Board and agency authorizations to operate that receive FedRAMP authorization from the FedRAMP Program Management Office shall be presumed adequate for use in agency authorizations of cloud computing products and services.

(2) INFORMATION SECURITY REQUIREMENTS.—The presumption under paragraph (1) does not modify or alter the responsibility of any agency to ensure compliance with subchapter II of chapter 35 for any cloud computing products or services used by the agency.

§ 3612. Roles and responsibilities of the Office of Management and Budget

The Director shall have the following duties:

(1) Issue guidance to ensure that an agency does not operate a Federal Government cloud computing service using Govern-

ment data without an authorization to operate issued by the agency that meets the requirements of subchapter II of chapter 35 and FedRAMP.

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

(3) Review, analyze, and update guidance on the adoption, security, and use of cloud computing services used by agencies.

(4) Ensure the Joint Authorization Board is in compliance with section 3609(c).

(5) Adjudicate disagreements between the Joint Authorization Board and cloud service providers seeking a provisional authorization to operate through the Joint Authorization Board.

(6) Promulgate regulations on the role of FedRAMP authorization in agency acquisition of cloud computing products and services that process unclassified information.

§ 3613. Authorization of appropriations for FEDRAMP

There is authorized to be appropriated $20,000,000 each year for the FedRAMP Program Management Office and the Joint Authorization Board.

§ 3614. Reports to Congress

Not later than 12 months after the date of the enactment of this section, and annually thereafter, the Director shall submit to the Committee on Oversight and Reform of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes the following:

(1) The status, efficiency, and effectiveness of FedRAMP Program Management Office and agencies during the preceding year in supporting the speed, effectiveness, sharing, reuse, and security of authorizations to operate for cloud computing products and services, including progress towards meeting the metrics adopted by the FedRAMP Program Management Office pursuant to section 3608(d) and the Joint Authorization Board pursuant to section 3609(c)(5).

(2) Data on agency use of provisional authorizations to operate issued by the Joint Authorization Board and agency sponsored authorizations that receive FedRAMP authorization by the FedRAMP Program Management Office.

(3) The length of time for the Joint Authorization Board to review applications for and issue provisional authorizations to operate.

(4) The length of time for the FedRAMP Program Management Office to review agency applications for and issue FedRAMP authorization.

(5) The number of provisional authorizations to operate issued by the Joint Authorization Board and FedRAMP authorizations issued by the FedRAMP Program Management Office for the previous year.

(6) A review of progress made during the preceding year in advancing automation techniques to securely automate FedRAMP processes and to accelerate reporting as described in this section.

(7) The number and characteristics of authorized cloud computing services in use at each agency consistent with guidance provided by the Director in section 3612.

§ 3615. Federal Secure Cloud Advisory Committee

(a) ESTABLISHMENT, PURPOSES, AND DUTIES.—

(1) ESTABLISHMENT.—There is established a Federal Secure Cloud Advisory Committee (referred to in this section as the "Committee") to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of cloud computing products and services to enable agency mission and administrative priorities.

(2) PURPOSES.—The purposes of the Committee are the following:

(A) To examine the operations of FedRAMP and determine ways that authorization processes can continuously be improved, including the following:

(i) Measures to increase agency re-use of provisional authorizations to operate issued by the Joint Authorization Board.

(ii) Proposed actions that can be adopted to reduce the cost of provisional authorizations to operate and FedRAMP authorizations for cloud service providers.

(iii) Measures to increase the number of provisional authorizations to operate or FedRAMP authorizations for cloud computing services offered by small businesses (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

(B) Collect information and feedback on agency compliance with and implementation of FedRAMP requirements.

(C) Serve as a forum that facilitates communication and collaboration among the FedRAMP stakeholder community.

(3) DUTIES.—The duties of the Committee are, at a minimum, the following:

(A) Provide advice and recommendations to the Administrator, the Joint Authorization Board, and to agencies on technical, financial, programmatic, and operational matters regarding secure adoption of cloud computing services.

(B) Submit reports as required.

(b) MEMBERS.—

(1) COMPOSITION.—The Committee shall be comprised of not more than 15 members who are qualified representatives from the public and private sectors, appointed by the Administrator, in consultation with the Administrator of the Office of Electronic Government, as follows:

(A) The Administrator or the Administrator's designee, who shall be the Chair of the Committee.

(B) At least 1 representative each from the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

(C) At least 2 officials who serve as the Chief Information Security Officer within an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

(D) At least 1 official serving as Chief Procurement Officer (or equivalent) in an agency, who shall be required to maintain such a position throughout the duration of their service on the Committee.

(E) At least 1 individual representing an independent assessment organization.

(F) No fewer than 5 representatives from unique businesses that primarily provide cloud computing services or products, including at least 2 representatives from a small business (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a))).

(G) At least 2 other government representatives as the Administrator determines to be necessary to provide sufficient balance, insights, or expertise to the Committee.

(2) DEADLINE FOR APPOINTMENT.—Each member of the Committee shall be appointed not later than 30 days after the date of the enactment of this Act.

(3) PERIOD OF APPOINTMENT; VACANCIES.—

(A) IN GENERAL.—Each non-Federal member of the Committee shall be appointed for a term of 3 years, except that the initial terms for members may be staggered 1, 2, or 3 year terms to establish a rotation in which one-third of the members are selected each year. Any such member may be appointed for not more than 2 consecutive terms.

(B) VACANCIES.—Any vacancy in the Committee shall not affect its powers, but shall be filled in the same manner in which the original appointment was made. Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office.

(c) MEETINGS AND RULES OF PROCEDURES.—

(1) MEETINGS.—The Committee shall hold not fewer than 3 meetings in a calendar year, at such time and place as determined by the Chair.

(2) INITIAL MEETING.—Not later than 120 days after the date of the enactment of this section, the Committee shall meet and begin the operations of the Committee.

(3) RULES OF PROCEDURE.—The Committee may establish rules for the conduct of the business of the Committee, if such rules are not inconsistent with this section or other applicable law.

(d) EMPLOYEE STATUS.—

(1) IN GENERAL.—A member of the Committee (other than a member who is appointed to the Committee in connection with another Federal appointment) shall not be considered an employee of the Federal Government by reason of any service as such a member, except for the purposes of section 5703 of title 5, relating to travel expenses.

(2) PAY NOT PERMITTED.—A member of the Committee covered by paragraph (1) may not receive pay by reason of service on the panel.

(e) APPLICABILITY TO THE FEDERAL ADVISORY COMMITTEE ACT.—Notwithstanding any other provision of law, the Federal Advisory

Committee Act (5 U.S.C. App.) shall apply to the Committee, except that section 14 of such Act shall not apply.

(f) HEARINGS AND EVIDENCE.—The Committee, or on the authority of the Committee, any subcommittee, may, for the purposes of carrying out this section, hold hearings, sit and act at such times and places, take testimony, receive evidence, and administer oaths.

(g) CONTRACTING.—The Committee, may, to such extent and in such amounts as are provided in appropriation Acts, enter into contracts to enable the Committee to discharge its duties under this section.

(h) INFORMATION FROM FEDERAL AGENCIES.—

(1) IN GENERAL.—The Committee is authorized to secure directly from any executive department, bureau, agency, board, commission, office, independent establishment, or instrumentality of the Government, information, suggestions, estimates, and statistics for the purposes of the Committee. Each department, bureau, agency, board, commission, office, independent establishment, or instrumentality shall, to the extent authorized by law, furnish such information, suggestions, estimates, and statistics directly to the Committee, upon request made by the Chair, the Chair of any subcommittee created by a majority of the Committee, or any member designated by a majority of the Committee.

(2) RECEIPT, HANDLING, STORAGE, AND DISSEMINATION.—Information may only be received, handled, stored, and disseminated by members of the Committee and its staff consistent with all applicable statutes, regulations, and Executive orders.

(i) ASSISTANCE FROM AGENCIES.—

(1) OTHER DEPARTMENTS AND AGENCIES.—In addition to the administration of the Committee by the General Services Administration, other agencies may provide to the Committee such services, funds, facilities, staff, and other support services as the head of the agency determines to be advisable and as is authorized by law.

(2) DETAIL OF EMPLOYEES.—Any Federal Government employee may be detailed to the Committee without reimbursement from the Committee, and such detailee shall retain the rights, status, and privileges of his or her regular employment without interruption.

(j) POSTAL SERVICES.—The Committee may use the United States mails in the same manner and under the same conditions as agencies.

(k) EXPERT AND CONSULTANT SERVICES.—The Committee is authorized to procure the services of experts and consultants in accordance with section 3109 of title 5, but at rates not to exceed the daily rate paid a person occupying a position at Level IV of the Executive Schedule under section 5315 of title 5.

(l) REPORTS.—

(1) INTERIM REPORTS.—The Committee may submit to the Administrator and Congress interim reports containing such findings, conclusions, and recommendations as have been agreed to by the Committee.

(2) ANNUAL REPORTS.—Not later than 18 months after the date of the enactment of this section, and annually thereafter, the Committee shall submit to the Administrator and Congress

a final report containing such findings, conclusions, and recommendations as have been agreed to by the Committee.

§ 3616. Definitions

(a) IN GENERAL.—Except as provided under subsection (b), the definitions under sections 3502 and 3552 apply to sections 3607 through this section.

(b) ADDITIONAL DEFINITIONS.—In sections 3607 through this section:

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

(2) AUTHORIZATION PACKAGE.—The term "authorization package"—

(A) means the essential information used to determine whether to authorize the operation of an information system or the use of a designated set of common controls; and

(B) at a minimum, includes the information system security plan, privacy plan, security control assessment, privacy control assessment, and any relevant plans of action and milestones.

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

(4) CLOUD SERVICE PROVIDER.—The term "cloud service provider" means an entity offering cloud computing services to agencies.

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

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

(7) FEDRAMP AUTHORIZATION.—The term "FedRAMP authorization" means a cloud computing product or service that has received an agency authorization to operate and has been approved by the FedRAMP Program Management Office to meet requirements and guidelines established by the FedRAMP Program Management Office.

(8) FEDRAMP PROGRAM MANAGEMENT OFFICE.—The term "FedRAMP Program Management Office" means the office that administers FedRAMP established under section 3608.

(9) INDEPENDENT ASSESSMENT ORGANIZATION.—The term "independent 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.

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

* * * * * * *

○