AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

I

116TH CONGRESS
1ST SESSION

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.

IN THE HOUSE OF REPRESENTATIVES

JULY 24, 2019

Mr. CONNOLLY (for himself and Mr. MEADOWS) introduced the following bill; which was referred to the Committee on Oversight and Reform

---

A BILL

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.

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 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.—There are established as components of FedRAMP the Joint Authorization Board and the Program Management Office, or such successor offices as the Administrator may determine.

"§ 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 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, including the role of cloud brokers and cloud service integrators;

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

''(C) oversee the administration of the Federal Secure Cloud Advisory Committee, established pursuant to section 3615; and

''(D) 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;

"(D) adjudicating disagreements between the Joint Authorization Board and cloud service providers seeking a provisional authorization to operate through the Joint Authorization Board; and

"(E) 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) 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.

''(2) Provide guidance to independent assessment organizations and oversee the execution of independent assessments in using and applying the requirements and guidelines adopted in paragraph (1).

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

''(4) 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.

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

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

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

''(8) Coordinate with the Department of Homeland Security to establish a framework for continuous monitoring and reporting required of agencies pursuant to section 3554.

''(9) Issue examples of security architectures to agencies and cloud computing services to better standardize and replicate secure configurations within a single cloud service and among cloud services.

''(10) 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 im-

prove the efficiency and effectiveness of the issuance of provisional authorizations to operate issued by the Joint Authorization Board and FedRAMP authorizations, including better control inheritance and 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 3553 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 3 security 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.

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

''(2) review and validate cloud computing services and independent assessment organization authorization packages;

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

''(4) 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

''(5) establish metrics and goals for reviews and activities associated with issuing provisional authorizations to operate.

''(d) DETERMINATIONS OF DEMAND FOR CLOUD COMPUTING SERVICES.—The Joint Authorization Board shall consult with the head of each agency 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 Administrator, in consultation with the Joint Authorization Board, shall determine the requirements for certification of independent assessment organizations. Such re-

quirements 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 3553;

''(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 Man-

agement 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, 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 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 issuing 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) 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 $25,000,000 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 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 each 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.—The Administrator shall establish within the General Services Administration the Federal Secure Cloud Advisory (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 to:

''(A) Examine the operations of FedRAMP and determine ways that authorization processes can continuously be improved.

''(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) No fewer than 5 representatives from 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))).

"(F) Any other 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 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 less 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) TRAVEL EXPENSES.—While away from their homes or regular places of business in the performance of services for the Committee, members of the Committee shall be allowed travel expenses, including per diem in lieu of subsistence, in the same manner as persons employed intermittently in the Government service are allowed expenses under section 5703(b) of title 5, United States Code.

''(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) GIFTS.—The Committee may accept, use, and dispose of gifts or donations of services or property.

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

''(l) 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.

''(m) VOLUNTEER SERVICES.—Notwithstanding section 1342 of title 31, the Committee may accept and use voluntary and uncompensated services as the Committee determines necessary.

''(n) 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.

''(o) SUNSET PROVISION.—The authority and obligations established by this section shall terminate on the

date that is five years after the date of the enactment of this section.

"§ 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 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.

''(4) 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.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means a non-Federal entity offering cloud computing services to agencies.

''(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 certified 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.

''(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.

''(11) SECURITY ARCHITECTURE.—The term 'security architecture' means a set of physical and logical security-relevant representations of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.''.

(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:

''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.''.

○