H.R.21 - FedRAMP Authorization Act

117th Congress (2021-2022)

Shown Here:
Referred in Senate (01/06/2021)

117TH CONGRESS
1ST SESSION

H. R. 21

IN THE SENATE OF THE UNITED STATES

JANUARY 6, 2021

Received; read twice and referred to the Committee on Homeland Security and Governmental Affairs

AN ACT

To enhance the innovation, security, and availability of cloud computing products and 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 products and 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 2021" 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 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 products and services that are within the jurisdiction of FedRAMP and that require a FedRAMP authorization or a FedRAMP provisional authorization;

"(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 products

and services pursuant to subsections (b) and (c) of section 3611, and appropriate oversight of continuous monitoring of cloud computing products and 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 necessary requirements for accreditation of third-party organizations seeking to be awarded accreditation as independent assessment organizations, including 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 products and 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) Review any authorization to operate issued by an agency to determine if the authorization meets the requirements and guidelines adopted in section 3609(c)(5).

"(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 under section 3553 and agency reports required under section 3554.

"(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 of 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 FedRAMP authorizations and FedRAMP provisional authorizations, including continuous monitoring of cloud computing products and services.

"(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.—The Joint Authorization Board 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 FEDRAMP PROVISIONAL AUTHORIZATIONS.—The Joint Authorization Board shall conduct security assessments of cloud computing products and services and issue FedRAMP provisional authorizations to cloud service providers that meet the requirements and guidelines established in subsection (c)(5).

"(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 products and services to be assessed by the Joint Authorization Board;

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

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

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

"(5) establish requirements and guidelines for security assessments of cloud computing products and 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 FedRAMP provisional authorizations and provide to the FedRAMP Program Management Office.

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

"(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 the accreditation of a third-party organization seeking to be accredited as an independent assessment organization, ensuring adequate implementation of section 3609. Such requirements may include developing or requiring certification programs for individuals employed by the third-party organization seeking accreditation. The Program Director of the FedRAMP Program Management Office shall accredit any third-party organization that meets the requirements for accreditation.

"(b) ASSESSMENT.—An independent assessment organization may assess, validate, and attest to the quality and compliance of security assessment materials provided by cloud service providers as part of the FedRAMP authorization or the FedRAMP provisional authorization process.

"§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 products and 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 FedRAMP authorization or FedRAMP provisional authorization in the cloud security repository established under section 3608(b)(8) before beginning the process to award a FedRAMP authorization or a FedRAMP provisional 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 a FedRAMP authorization or FedRAMP provisional authorization, 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 agency authorization to operate, the head of the 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 a FedRAMP authorization or FedRAMP provisional authorization shall be presumed adequate for use in an agency authorization to operate 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 product or service using Government data without an authorization to operate issued by the agency that meets the requirements of subchapter II of chapter 35 and the FedRAMP authorization or FedRAMP provisional authorization.

"(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 FedRAMP provisional authorization.

"(6) Promulgate regulations on the role of FedRAMP authorizations and FedRAMP provisional authorizations 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; GAO Report

"(a) 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 FedRAMP authorizations and FedRAMP provisional authorizations.

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

"(4) The average length of time for the FedRAMP Program Management Office to review authorizations to operate.

"(5) The number of FedRAMP authorizations and FedRAMP provisional authorizations issued 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 products and services in use at each agency consistent with guidance provided by the Director in section 3612.

"(8) The cost incurred by agencies and cloud service providers related to the issuance of FedRAMP authorizations and FedRAMP provisional authorizations, including information responsive to the report required in subsection (b).

"(b) GAO REPORT.—Not later than 6 months after the date of the enactment of this section, the Comptroller General of the United States shall publish a report that includes an assessment of the cost incurred by agencies and cloud service providers related to the issuance of FedRAMP authorizations and FedRAMP provisional authorizations.

"§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 FedRAMP provisional authorizations.

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

"(iii) Measures to increase the number of FedRAMP authorizations and FedRAMP provisional 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, to 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 products and services.

"(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 one representative each from the Cybersecurity and Infrastructure Security Agency and the National Institute of Standards and Technology.

"(C) At least two 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 one 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 one individual representing an independent assessment organization.

"(F) No fewer than five representatives from unique businesses that primarily provide cloud computing services or products, including at least two 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 two 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 section.

"(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 three 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 Committee.

"(e) APPLICABILITY TO THE FEDERAL ADVISORY COMMITTEE ACT.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Committee.

"(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) 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 products or 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 certification that a cloud computing product or service received from an agency that provides an authorization to operate and the FedRAMP Program Management Office has determined the product or service has completed the FedRAMP authorization process.

"(8) FEDRAMP PROGRAM MANAGEMENT OFFICE.—The term 'FedRAMP Program Management Office' means the office that administers FedRAMP established under section 3607(b).

"(9) FEDRAMP PROVISIONAL AUTHORIZATION.—The term 'FedRAMP provisional authorization' means a certification that a cloud computing product or service has received from the Joint Authorization Board

that approves a provisional authorization to operate.

"(10) 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 and their products or services.

"(11) JOINT AUTHORIZATION BOARD.—The term 'Joint Authorization Board' means the Joint Authorization Board established under section 3607(b).".

(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:

(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.

Passed the House of Representatives January 5, 2021.

Attest: CHERYL L. JOHNSON,
Clerk.