117TH CONGRESS
2D SESSION

H.R.

To amend chapter 36 of title 44, United States Code, to improve the
cybersecurity of the Federal Government, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To amend chapter 36 of title 44, United States Code, to improve the cybersecurity of the Federal Government, and for other purposes.

1 Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,
3 SECTION 1. SHORT TITLE.
4 This Act may be cited as the “FedRAMP Authorization Act”.
5 SEC. 2. FINDINGS.
6 Congress finds the following:
(1) Ensuring that the Federal Government can securely leverage cloud computing products and services is key to expediting the modernization of legacy information technology systems, increasing cybersecurity within and across departments and agencies, and supporting the continued leadership of the United States in technology innovation and job creation.

(2) According to independent analysis, as of calendar year 2019, the size of the cloud computing market had tripled since 2004, enabling more than 2,000,000 jobs and adding more than $200,000,000,000 to the gross domestic product of the United States.

(3) The Federal Government, across multiple presidential administrations and Congresses, has continued to support the ability of agencies to move to the cloud, including through—

(A) President Barack Obama’s "Cloud First Strategy";

(B) President Donald Trump’s "Cloud Smart Strategy";

(C) the prioritization of cloud security in Executive Order 14028 (86 Fed. Reg. 26633; relating to improving the nation’s cybersecurity—
rity), which was issued by President Joe Biden;
and
(D) more than a decade of appropriations
and authorization legislation that provides
agencies with relevant authorities and appro-
priations to modernize on-premises information
technology systems and more readily adopt
cloud computing products and services.
(4) Since it was created in 2011, the Federal
Risk and Authorization Management Program (re-
ferred to in this section as “FedRAMP”) at the
General Services Administration has made steady
and sustained improvements in supporting the se-
cure authorization and reuse of cloud computing
products and services within the Federal Gover-
ment, including by reducing the costs and burdens
on both agencies and cloud companies to quickly and
securely enter the Federal market.
(5) According to data from the General Services
Administration, as of the end of fiscal year 2021,
there were 239 cloud providers with FedRAMP au-
thorizations, and those authorizations had been re-
used more than 2,700 times across various agencies.
(6) Providing a legislative framework for
FedRAMP and new authorities to the General Serv-
ices Administration, the Office of Management and
Budget, and Federal agencies will—

(A) improve the speed at which new cloud
computing products and services can be se-
curely authorized;

(B) enhance the ability of agencies to ef-
effectively evaluate FedRAMP authorized pro-
viders for reuse;

(C) reduce the costs and burdens to cloud
providers seeking a FedRAMP authorization;

and

(D) provide for more robust transparency
and dialogue between industry and the Federal
Government to drive stronger adoption of se-
cure cloud capabilities, create jobs, and reduce
wasteful legacy information technology.

SEC. 3. TITLE 44 AMENDMENTS.

(a) AMENDMENT.—Chapter 36 of title 44, United
States Code, is amended by adding at the end the fol-
lowing:

§ 3607. Definitions

(a) IN GENERAL.—Except as provided under sub-
section (b), the definitions under sections 3502 and 3552
apply to this section through section 3616.
"(b) ADDITIONAL DEFINITIONS.—In this section through section 3616:

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

"(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ‘appropriate congressional committees’ means the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives.

"(3) AUTHORIZATION TO OPERATE; FEDERAL INFORMATION.—The terms ‘authorization to operate' and ‘Federal information’ have the meaning given those term in Circular A–130 of the Office of Management and Budget entitled ‘Managing Information as a Strategic Resource’, or any successor document.

"(4) CLOUD COMPUTING.—The term ‘cloud computing’ has the meaning given the term in Special Publication 800–145 of the National Institute of Standards and Technology, or any successor document.

"(5) CLOUD SERVICE PROVIDER.—The term ‘cloud service provider’ means an entity offering cloud computing products or services to agencies.
“(6) **FedRAMP.**—The term ‘FedRAMP’ means the Federal Risk and Authorization Management Program established under section 3608.

“(7) **FedRAMP AUTHORIZATION.**—The term ‘FedRAMP authorization’ means a certification that a cloud computing product or service has—

“(A) completed a FedRAMP authorization process, as determined by the Administrator; or

“(B) received a FedRAMP provisional authorization to operate, as determined by the FedRAMP Board.

“(8) **FedRAMP AUTHORIZATION PACKAGE.**—The term ‘FedRAMP authorization package’ means the essential information that can be used by an agency to determine whether to authorize the operation of an information system or the use of a designated set of common controls for all cloud computing products and services authorized by FedRAMP.

“(9) **FedRAMP BOARD.**—The term ‘FedRAMP Board’ means the board established under section 3610.

“(10) **INDEPENDENT ASSESSMENT SERVICE.**—The term ‘independent assessment service’ means a third-party organization accredited by the Adminis-
trator to undertake conformity assessments of cloud
service providers and the products or services of
cloud service providers.

“(11) SECRETARY.—The term ‘Secretary’
means the Secretary of Homeland Security.

§ 3608. Federal Risk and Authorization Management
Program

“There is established within the General Services Ad-
ministration the Federal Risk and Authorization Manage-
ment Program. The Administrator, subject to section
3614, shall establish a Government-wide program that
provides a standardized, reusable approach to security as-
essment and authorization for cloud computing products
and services that process unclassified information used by
agencies.

§ 3609. Roles and responsibilities of the General
Services Administration

“(a) ROLES AND RESPONSIBILITIES.—The Adminis-
trator shall—

“(1) in consultation with the Secretary, develop,
coordinate, and implement a process to support
agency review, reuse, and standardization, where ap-
propriate, of security assessments of cloud com-
puting products and services, including, as appro-
priate, oversight of continuous monitoring of cloud
computing products and services, pursuant to guidance issued by the Director pursuant to section 3614;

“(2) establish processes and identify criteria consistent with guidance issued by the Director under section 3614 to make a cloud computing product or service eligible for a FedRAMP authorization and validate whether a cloud computing product or service has a FedRAMP authorization;

“(3) develop and publish templates, best practices, technical assistance, and other materials to support the authorization of cloud computing products and services and increase the speed, effectiveness, and transparency of the authorization process, consistent with standards and guidelines established by the Director of the National Institute of Standards and Technology and relevant statutes;

“(4) establish and update guidance on the boundaries of FedRAMP authorization packages to enhance the security and protection of Federal information and promote transparency for agencies and users as to which services are included in the scope of a FedRAMP authorization;
“(5) grant FedRAMP authorizations to cloud computing products and services consistent with the guidance and direction of the FedRAMP Board;

“(6) establish and maintain a public comment process for proposed guidance and other FedRAMP directives that may have a direct impact on cloud service providers and agencies before the issuance of such guidance or other FedRAMP directives;

“(7) coordinate with the FedRAMP Board, the Director of the Cybersecurity and Infrastructure Security Agency, and other entities identified by the Administrator, with the concurrence of the Director and the Secretary, to establish and regularly update a framework for continuous monitoring under section 3553;

“(8) provide a secure mechanism for storing and sharing necessary data, including FedRAMP authorization packages, to enable better reuse of such packages across agencies, including making available any information and data necessary for agencies to fulfill the requirements of section 3613;

“(9) provide regular updates to applicant cloud service providers on the status of any cloud computing product or service during an assessment process;
“(10) regularly review, in consultation with the FedRAMP Board—

“(A) the costs associated with the independent assessment services described in section 3611; and

“(B) the information relating to foreign interests submitted pursuant to section 3612;

“(11) in coordination with the Director of the National Institute of Standards and Technology, the Director, the Secretary, and other stakeholders, as appropriate, determine the sufficiency of underlying standards and requirements to identify and assess the provenance of the software in cloud services and products;

“(12) support the Federal Secure Cloud Advisory Committee established pursuant to section 3616; and

“(13) take such other actions as the Administrator may determine necessary to carry out FedRAMP.

“(b) WEBSITE.—

“(1) IN GENERAL.—The Administrator shall maintain a public website to serve as the authoritative repository for FedRAMP, including the timely publication and updates for all relevant information,
guidance, determinations, and other materials re-
quired under subsection (a).

“(2) CRITERIA AND PROCESS FOR FEDRAMP
AUTHORIZATION PRIORITIES.—The Administrator
shall develop and make publicly available on the
website described in paragraph (1) the criteria and
process for prioritizing and selecting cloud com-
puting products and services that will receive a
FedRAMP authorization, in consultation with the
FedRAMP Board and the Chief Information Offi-
cers Council.

“(c) EVALUATION OF AUTOMATION PROCEDURES.—

“(1) IN GENERAL.—The Administrator, in co-
ordination with the Secretary, shall assess and
evaluate available automation capabilities and proce-
dures to improve the efficiency and effectiveness of
the issuance of FedRAMP authorizations, including
continuous monitoring of cloud computing products
and services.

“(2) MEANS FOR AUTOMATION.—Not later than
1 year after the date of enactment of this section,
and updated regularly thereafter, the Administrator
shall establish a means for the automation of secu-

rity assessments and reviews.
“(d) Metrics for Authorization.—The Administrator 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.

§ 3610. FedRAMP Board

“(a) Establishment.—There is established a FedRAMP Board to provide input and recommendations to the Administrator regarding the requirements and guidelines for, and the prioritization of, security assessments of cloud computing products and services.

“(b) Membership.—The FedRAMP Board shall consist of not more than 7 senior officials or experts from agencies appointed by the Director, in consultation with the Administrator, from each of the following:

“(1) The Department of Defense.


“(3) The General Services Administration.

“(4) Such other agencies as determined by the Director, in consultation with the Administrator.
“(c) Qualifications.—Members of the FedRAMP Board appointed under subsection (b) shall have technical expertise in domains relevant to FedRAMP, such as—

“(1) cloud computing;
“(2) cybersecurity;
“(3) privacy;
“(4) risk management; and
“(5) other competencies identified by the Director to support the secure authorization of cloud services and products.

“(d) Duties.—The FedRAMP Board shall—

“(1) in consultation with the Administrator, serve as a resource for best practices to accelerate the process for obtaining a FedRAMP authorization;
“(2) establish and regularly update requirements and guidelines for security authorizations of cloud computing products and services, consistent with standards and guidelines established by the Director of the National Institute of Standards and Technology, to be used in the determination of FedRAMP authorizations;
“(3) monitor and oversee, to the greatest extent practicable, the processes and procedures by which agencies determine and validate requirements for a FedRAMP authorization, including periodic review
of the agency determinations described in section 3613(b);

"(4) ensure consistency and transparency between agencies and cloud service providers in a manner that minimizes confusion and engenders trust; and

"(5) perform such other roles and responsibilities as the Director may assign, with concurrence from the Administrator.

"(e) DETERMINATIONS OF DEMAND FOR CLOUD COMPUTING PRODUCTS AND SERVICES.—The FedRAMP Board may consult with the Chief Information Officers Council to establish a process, which may be made available on the website maintained under section 3609(b), for prioritizing and accepting the cloud computing products and services to be granted a FedRAMP authorization.

"§3611. Independent assessment

"The Administrator may determine whether FedRAMP may use an independent assessment service to analyze, validate, and attest to the quality and compliance of security assessment materials provided by cloud service providers during the course of a determination of whether to use a cloud computing product or service.
§ 3612. Declaration of foreign interests

(a) In General.—An independent assessment service that performs services described in section 3611 shall annually submit to the Administrator information relating to any foreign interest, foreign influence, or foreign control of the independent assessment service.

(b) Updates.—Not later than 48 hours after there is a change in foreign ownership or control of an independent assessment service that performs services described in section 3611, the independent assessment service shall submit to the Administrator an update to the information submitted under subsection (a).

(c) Certification.—The Administrator may require a representative of an independent assessment service to certify the accuracy and completeness of any information submitted under this section.

§ 3613. 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 3614—

(1) promote the use of cloud computing products and services that meet FedRAMP security requirements and other risk-based performance requirements as determined by the Director, in consultation with the Secretary;
“(2) confirm whether there is a FedRAMP authorization in the secure mechanism provided under section 3609(a)(8) before beginning the process of granting a FedRAMP authorization for a cloud computing product or service;

“(3) to the extent practicable, for any cloud computing product or service the agency seeks to authorize that has received a FedRAMP authorization, use the existing assessments of security controls and materials within any FedRAMP authorization package for that cloud computing product or service; and

“(4) provide to the Director data and information required by the Director pursuant to section 3614 to determine how agencies are meeting metrics established by the Administrator.

“(b) ATTESTATION.—Upon completing an assessment or authorization activity with respect to a particular cloud computing product or service, if an agency determines that the information and data the agency has reviewed under paragraph (2) or (3) of subsection (a) is wholly or substantially deficient for the purposes of performing an authorization of the cloud computing product or service, the head of the agency shall document as part of the resulting FedRAMP authorization package the reasons for this determination.
“(c) Submission of Authorizations to Operate Required.—Upon issuance of an agency authorization to operate based on a FedRAMP authorization, the head of the agency shall provide a copy of its authorization to operate letter and any supplementary information required pursuant to section 3609(a) to the Administrator.

“(d) Submission of Policies Required.—Not later than 180 days after the date on which the Director issues guidance in accordance with section 3614(1), the head of each agency, acting through the chief information officer of the agency, shall submit to the Director all agency policies relating to the authorization of cloud computing products and services.

“(e) Presumption of Adequacy.—

“(1) In General.—The assessment of security controls and materials within the authorization package for a FedRAMP 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—

“(A) the responsibility of any agency to ensure compliance with subchapter II of chapter
35 for any cloud computing product or service
used by the agency; or
“(B) the authority of the head of any
agency to make a determination that there is a
demonstrable need for additional security re-
quirements beyond the security requirements
included in a FedRAMP authorization for a
particular control implementation.

“§3614. Roles and responsibilities of the Office of
Management and Budget
“The Director shall—
“(1) in consultation with the Administrator and
the Secretary, issue guidance that—
“(A) specifies the categories or characteris-
tics of cloud computing products and services
that are within the scope of FedRAMP;
“(B) includes requirements for agencies to
obtain a FedRAMP authorization when oper-
ating a cloud computing product or service de-
scribed in subparagraph (A) as a Federal infor-
mation system; and
“(C) encompasses, to the greatest extent
practicable, all necessary and appropriate cloud
computing products and services;
“(2) issue guidance describing additional responsibilities of FedRAMP and the FedRAMP Board to accelerate the adoption of secure cloud computing products and services by the Federal Government;

“(3) in consultation with the Administrator, establish a process to periodically review FedRAMP authorization packages to support the secure authorization and reuse of secure cloud products and services;

“(4) oversee the effectiveness of FedRAMP and the FedRAMP Board, including the compliance by the FedRAMP Board with the duties described in section 3610(d); and

“(5) to the greatest extent practicable, encourage and promote consistency of the assessment, authorization, adoption, and use of secure cloud computing products and services within and across agencies.

§3615. Reports to Congress; GAO report

“(a) REPORTS TO CONGRESS.—Not later than 1 year after the date of enactment of this section, and annually thereafter, the Director shall submit to the appropriate congressional committees a report that includes the fol-
“(1) During the preceding year, the status, efficiency, and effectiveness of the General Services Administration under section 3609 and agencies under section 3613 and in supporting the speed, effectiveness, sharing, reuse, and security of authorizations to operate for secure cloud computing products and services.

“(2) Progress towards meeting the metrics required under section 3609(d).

“(3) Data on FedRAMP authorizations.

“(4) The average length of time to issue FedRAMP authorizations.

“(5) The number of FedRAMP authorizations submitted, issued, and denied for the preceding year.

“(6) A review of progress made during the preceding year in advancing automation techniques to securely automate FedRAMP processes and to accelerate reporting under 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 under section 3614.

“(8) A review of FedRAMP measures to ensure the security of data stored or processed by cloud service providers, which may include—
“(A) geolocation restrictions for provided products or services;

“(B) disclosures of foreign elements of supply chains of acquired products or services;

“(C) continued disclosures of ownership of cloud service providers by foreign entities; and

“(D) encryption for data processed, stored, or transmitted by cloud service providers.

“(b) GAO REPORT.—Not later than 180 days after the date of enactment of this section, the Comptroller General of the United States shall report to the appropriate congressional committees an assessment of the following:

“(1) The costs incurred by agencies and cloud service providers relating to the issuance of FedRAMP authorizations.

“(2) The extent to which agencies have processes in place to continuously monitor the implementation of cloud computing products and services operating as Federal information systems.

“(3) How often and for which categories of products and services agencies use FedRAMP authorizations.

“(4) The unique costs and potential burdens incurred by cloud computing companies that are small
business concerns (as defined in section 3(a) of the Small Business Act (15 U.S.C. 632(a)) as a part of the FedRAMP authorization process.

§3616. 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 reuse of FedRAMP authorizations.

"(ii) Proposed actions that can be adopted to reduce the burden, confusion, and cost associated with FedRAMP authorizations for cloud service providers.
“(iii) Measures to increase the number of FedRAMP authorizations for cloud computing products and services offered by small businesses concerns (as defined by section 3(a) of the Small Business Act (15 U.S.C. 632(a)).

“(iv) Proposed actions that can be adopted to reduce the burden and cost of FedRAMP authorizations for agencies.

“(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 include providing advice and recommendations to the Administrator, the FedRAMP Board, and 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 consulta-
tion with the Director, as follows:

"(A) The Administrator or the Administra-
tor'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 serv-

ice on the Committee.

"(D) At least 1 official serving as Chief
Procurement Officer (or equivalent) in an agen-
cy, who shall be required to maintain such a po-

sition throughout the duration of their service
on the Committee.

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

"(F) At least 5 representatives from
unique businesses that primarily provide cloud
computing services or products, including at
least 2 representatives from a small business
concern (as defined by section 3(a) of the Small
Business Act (15 U.S.C. 632(a))).

“(G) At least 2 other representatives of the
Federal Government as the Administrator de-
determines 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 90 days after the date of 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 origi-

onal appointment was made. Any member ap-
pointed 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 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) DETAIL OF EMPLOYEES.—Any Federal Government employee may be detailed to the Committee without reimbursement from the Committee, and such detailer shall retain the rights, status, and privileges of his or her regular employment without interruption.

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

“(h) 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 540 days after the date of enactment of this section, and annually thereafter, the Committee shall submit to the Administrator and Congress a report containing
such findings, conclusions, and recommendations as
have been agreed to by the Committee.”.

(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 fol-
lowing new items:

“3607. Definitions.
“3610. FedRAMP Board.
“3612. Declaration of foreign interests.
“3613. Roles and responsibilities of agencies.
“3614. Roles and responsibilities of the Office of Management and Budget.
“3615. Reports to Congress; GAO report.
“3616. Federal Secure Cloud Advisory Committee.”.

(c) SUNSET.—

(1) IN GENERAL.—Effective on the date that is
5 years after the date of enactment of this Act,
chapter 36 of title 44, United States Code, is
amended by striking sections 3607 through 3616.

(2) CONFORMING AMENDMENT.—Effective on
the date that is 5 years after the date of enactment
of this Act, the table of sections for chapter 36 of
title 44, United States Code, is amended by striking
the items relating to sections 3607 through 3616.

(d) RULE OF CONSTRUCTION.—Nothing in this sec-

tion or any amendment made by this section shall be con-

strued as altering or impairing the authorities of the Di-
rector of the Office of Management and Budget or the
1 Secretary of Homeland Security under subchapter II of
2 chapter 35 of title 44, United States Code.