Calendar No. 383

117TH CONGRESS *2d Session*	SENATE	REPORT 117–115

FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 3099

TO AMEND TITLE 44, UNITED STATES CODE, TO ESTABLISH THE FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM WITHIN THE GENERAL SERVICES ADMINISTRATION, AND FOR OTHER PURPOSES

MAY 24, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
29–010 WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
LENA C. CHANG, *Director of Governmental Affairs*
MATTHEW T. CORNELIUS, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
AMANDA H. NEELY, *Minority Director of Governmental Affairs and General Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 383

117TH CONGRESS *2d Session* | SENATE | REPORT 117–115

FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS ACT OF 2021

MAY 24, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 3099]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3099) to amend title 44, United States Code, to establish the Federal Risk and Authorization Management Program within the General Services Administration, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 3099, the *Federal Secure Cloud Improvement and Jobs Act of 2021*, provides a statutory framework for the Federal Risk and Authorization Management Program (FedRAMP) to make the program more accountable and transparent and help ensure that agencies' processes of moving safely to the cloud are streamlined and efficient. As cloud computing technology continues its growth in our society and economy, it is important that federal agencies

quickly, securely, and effectively adopt these capabilities to improve digital service delivery and protect against malicious foreign threats.

S. 3099 would codify and reform the FedRAMP program at the General Services Administration (GSA) to ensure continuous growth in the number of cloud service providers (CSP) securely authorized in government, empower greater reuse of CSPs across agencies, and strengthen transparency measures to promote engagement and consensus recommendations from leaders in both industry and government that will accelerate cloud adoption. This bill would also ensure that CSPs and independent assessment services are protected from foreign threats by requiring additional steps to mitigate any malicious activity and increase reporting transparency to the government. S. 3099 also creates new requirements for agencies to affirmatively leverage high-quality security authorization packages rather than forcing CSPs to perform duplicative and costly work that slows agency efforts to modernize their information technology (IT).

Finally, S. 3099 provides for stronger oversight authorities of agency cloud computing processes and protocols by the Office of Management and Budget (OMB) and creates a Federal Secure Cloud Advisory Committee, comprising IT and cybersecurity leaders from both industry and the public sector, to provide recommendations to the GSA Administrator for improving the FedRAMP program and the government's adoption of cloud capabilities.

II. Background and Need for the Legislation

FedRAMP is a government-wide program at GSA, established pursuant to a memorandum issued to all agencies by OMB in 2011.[1] FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP's goals are to:

- Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations;
- Achieve consistent security authorizations using a baseline set of agreed-upon standards for cloud product approval; and
- Ensure consistent application of existing security practices.

As of today, there are 260 authorized CSPs, 67 CSPs in the process of receiving authorizations, and an additional 32 CSPs deemed ready by independent third party assessment organizations (3PAO).[2] Of the 240 CSPs already authorized, agencies have reused them over 2,700 times. Reuse of authorized CSPs has the potential to reduce time, cost, and burden to both agencies and industry partners.

While GSA has made substantial improvements in the operations, management, and execution of the FedRAMP program, creating a strong legislative foundation that addresses both the current challenges and future opportunities for secure cloud adoption in the federal government is vital to our national security interests

[1] Federal Risk and Authorization Management Program (FedRAMP), Home Page (www.fedramp.gov) (accessed January 3, 2022) (hereinafter "FedRAMP Website"); Office of Management and Budget, Memorandum from Steven Van Roekel to Chief Information Officers, *Security Authorization for Information Systems in Cloud Computing Environments* (Dec. 8, 2011).

[2] FedRAMP Website at Home Page.

and to our government's ability to more effectively deliver critical programs. To date, GSA has managed the FedRAMP program as one of many government-wide programs and services funded by the Federal Citizen Services Fund.[3] S. 3099 addresses key challenges surrounding secure cloud adoption in government by reducing costs, improving the speed of cloud adoption, promoting greater competition, enhancing the ability of the government to mitigate malicious threats of foreign control or influence of CSPs or independent assessment services, and bringing needed transparency to the cloud authorization, adoption, and reuse policies and processes for federal agencies. With the increase in both oversight and operational authorities for the FedRAMP program proposed in S. 3099, it is important that the program receive sufficient funding in the coming years to sufficiently address these new requirements.

III. Legislative History

Chairman Gary Peters (D–MI) introduced S. 3099 on October 28, 2021, with Senators Hawley (R–MO), Hassan (D–NH), and Daines (R–MT) as cosponsors. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3099 at a business meeting on December 15, 2021. During the business meeting, Chairman Peters, along with Senators Hawley, Hassan, and Portman (R–OH) offered a modified substitute amendment to S. 3099, which was adopted by unanimous consent. The modified substitute amendment removed a section that authorized appropriations for GSA to administer the FedRAMP program. Senator Ossoff (D–GA) offered an amendment, as modified, to the substitute, as modified, which was adopted by voice vote. The Ossoff amendment extended some of the regular reporting requirements for the FedRAMP program to include issues such as supply chain security and foreign threats around cloud service providers. S. 3099 was ordered reported favorably by voice vote as amended by the Peters-Hawley-Hassan-Portman substitute amendment as modified and the Ossoff amendment as modified. Senators present for the vote were: Peters, Carper, Hassan, Sinema, Rosen, Ossoff, Portman, Lankford, Romney, Scott, and Hawley.

IV. Section-by-Section Analysis of the Bill, as Reported

Section 1. Short title

This section designates the name of the bill as the "Federal Secure Cloud Improvement and Jobs Act of 2021."

Section 2. Findings

This section identifies congressional findings that the secure adoption of cloud technologies by federal agencies expedites the modernization of legacy information technologies, improves cybersecurity, and supports United States leadership in technology innovation. The section also finds that improving the adoption of cloud technologies has been a priority for multiple Administrations and Congresses and that the continued expansion of new and emerging

[3] General Services Administration Fiscal Year 2022 Budget Justification (https://www.gsa.gov/cdnstatic/20_FY_2022_CJ_Full_GSA_Narrative_v2_optimized.pdf) (accessed May 2, 2022).

cloud technologies supports the American economy and creates American jobs. Finally, the section finds that the Federal Risk Authorization and Management Program (FedRAMP) has been effective in supporting the secure adoption of cloud technologies by Federal agencies, but that legislative reforms are needed to improve management of the program and to ensure that agencies can more quickly, securely, and effectively leverage cloud technologies while reducing costs for both industry and taxpayers.

Section 3. Title 44 amendments

Subsection (a) amends Chapter 36 of Title 44 and creates the following new sections:

Section 3607 defines "Administrator," "appropriate congressional committees," "authorization to operate/federal information," "cloud computing," "cloud service provider," "FedRAMP," "FedRAMP authorization," "FedRAMP authorization package," "FedRAMP board," "independent assessment service," and "Secretary."

This section also stipulates that the definitions in Chapters 3502 and 3552 of Title 44 apply to the newly created Sections 3607 through 3616 of that title.

Section 3608 establishes the Federal Authorization Risk and Management Program (FedRAMP) in the General Services Administration (GSA).

Section 3609 provides the roles and responsibilities of the GSA Administrator. The section requires that the Administrator establish criteria, in coordination with the Director of the Office of Management and Budget (OMB) to define the types of cloud service providers (CSPs) that are eligible for FedRAMP certification and to coordinate with the Secretary to implement a process for agencies to review, certify, and assess the security of authorization package for CSPs.

The section provides additional authorities to the Administrator, including to: support the management of the Federal Secure Cloud Advisory Committee (created in Section 3616 of the legislation); grant authorization for CSPs consistent with oversight by the FedRAMP Board; provide for a public comment process for all guidance issued by GSA for the FedRAMP program; provide a secure repository to collect all CSP security packages authorized by GSA or federal agencies; coordinate with the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to ensure appropriate continuous monitoring for all authorized CSPs; and regularly review costs associated with the use of independent assessment services (created in Section 3611 of the legislation) and information related for foreign interests (created in Section 3612).

Lastly, the section requires the Administrator to maintain a centralized website for all FedRAMP information, guidance, determinations, and other materials relevant to Section 3609 and to establish metrics and measures for the automation of CSP authorizations, including reporting annually to Congress on the effectives of such metrics and measures.

Section 3610 establishes the FedRAMP Board, made up of 7 subject matter experts from across the Federal government, to help oversee the processes and procedures by which agencies authorize CSPs and provide recommendations for improving the outcomes of the FedRAMP Program. This section also defines the qualifications

for serving on the Board and establishes their duties, including regularly establishing and updating requirements and guidelines for security authorizations of CSPs and monitoring and overseeing processes and procedures by which agencies determine and validate requirements for a FedRAMP authorization. Finally, this section requires the Board to consult with the Federal Chief Information Officers Council to prioritize and accept CSPs for a FedRAMP authorization.

Section 3611 allows the Administrator to use independent assessment services to analyze, validate, and attest to the quality and compliance of CSP security materials during the course of an authorization.

Section 3612 requires that any independent assessment service used by the Administrator annually submit information to the Administrator regarding foreign ownership, influence, or control. This section also requires that any independent assessment service in use by the Administrator shall report any changes relating to foreign ownership, influence, or control to the Administrator not later than 48 hours after any such change has occurred and that the Administrator then certify any information provided by the independent assessment service.

Section 3613 establishes requirements for all agencies that authorize CSPs, pursuant to guidance issued by the OMB Director. In particular, this section requires agencies to first determine whether a security package already exists for any CSP which the agency seeks to authorize and, if so, use the already existing security package information and materials, to the greatest extent practicable, to authorize the CSP for use in that agency. This section requires all agencies who review the security package materials for any currently authorized CSPs to attest to the Director if the security package, or any materials or information therein, are wholly or substantially deficient for their purposes. This section requires all agencies that authorize CSPs to provide their particular security package information to the Administrator and, within 180 days of enactment, provide the Director all agency policies relating to the authorization of CSPs.

Lastly, this section creates a "presumption of adequacy" which says that all assessment of security controls and materials in any FedRAMP authorization shall be presumed adequate for use at any agency. The section also provides that the presumption of adequacy does not modify or alter agency responsibilities of the requirements of Subchapter II of Chapter 35, nor does it preclude an agency from requiring additional security requirements for any FedRAMP authorization.

Section 3614 creates authorities for the OMB Director, including the requirement that the Director consult with the Administrator and the Secretary when issuing guidance on specific categories and characteristics of CSPs that are within the scope of FedRAMP and requirements for agencies to obtain a FedRAMP authorization for all CSPs that are defined as federal information systems. This section also requires the Director to issue guidance describing additional authorities of the Administrator and FedRAMP Board to accelerate the secure adoption of CSPs in government, establish a process to regularly review all CSP authorizations in coordination with the Administrator, and to the greatest extent practicable, pro-

mote consistency of the assessment, authorization, adoption, and use of secure cloud computing products and services within and across agencies.

Section 3615 establishes annual reporting requirements by the Administration to Congress and requires a report by the Government Accountability Office (GAO).

Section 3616 creates the Federal Secure Cloud Advisory Committee (Committee) to ensure effective and ongoing coordination of agency adoption, use, authorization, monitoring, acquisition, and security of CSPs to enable agency mission and administrative priorities. The section establishes purposes for the Committee including examining how GSA and agencies can continuously improve their assessment and authorizations of CSPs, collect information and feedback on agency compliance with and implementation of FedRAMP requirements, and to serve as a forum to ensure collaboration and communication among the various FedRAMP stakeholders.

The section authorizes the Committee to be no more than 15 members comprising: the Administrator (who serves as Chair); at least 1 representative each from CISA and the National Institute of Standards and Technology; at least 2 officials who serve as Chief Information Security Officers (or equivalent) at an agency; at least 1 official who serves as Chief Procurement Officer (or equivalent) at an agency; at least 1 representative from an independent assessment service; and at least 5 representatives from industry stakeholders including at least 2 representatives designated as small businesses. The section defines requirements for Committee meetings and rules of procedures, employment status of representatives, the use of postal services by or the detail of federal employees to the Committee, and requirements for interim and annual reports. Lastly, this section requires the Committee be subject to the Federal Advisory Commission Act (5. U.S.C. App) except for Section 14 thereof.

Subsection (b) provides a technical and conforming amendment that establishes titles for the new sections created in Chapter 36 of Title 44.

Subsection (c) provides for a five year sunset to the Act and all amendments made pursuant to its passage.

Subsection (d) provides a rule of construction to stipulate that none of the amendments in this Act otherwise alter of impair the authorities of the OMB or the Secretary of the Department of Homeland Security provided under Subchapter II of Chapter 35 of Title 44.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 24, 2022.

Hon. GARY PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 3099, the Federal Secure Cloud Improvement and Jobs Act of 2021.

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.

S. 3099, Federal Secure Cloud Improvement and Jobs Act of 2021
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on December 15, 2021

By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	50	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 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000

S. 3099 would codify and expand the responsibilities of the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration (GSA). The bill would establish a standardized approach to acquiring and using security assessment and cloud-computing products and services. The bill also would establish the Federal Secure Cloud Advisory Committee to examine how the assessment and selection processes could be improved.

FedRAMP is currently part of GSA's Federal Citizens Services Fund which provides funds to federal agencies to build capacity for conducting activities electronically. The fund received $55 million in 2021. Using information from GSA regarding the FedRAMP program as well as the cost of other advisory committees, CBO estimates that implementing S. 3099 would cost about $50 million over the 2022–2026 period, assuming appropriation of the estimated amounts. CBO estimates that most of that cost would be to automate security assessments and to adopt new oversight procedures

required under the bill. There would be small costs each year to establish and operate the advisory committee.

The costs of the legislation (detailed in Table 1) fall within budget function 800 (general government). CBO expects that the bill will be enacted late in fiscal year 2022 and thus any costs in that year would be insignificant.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 3099

	By fiscal year, millions of dollars—					
	2022	2023	2024	2025	2026	2022–2026
Estimated Authorization	*	11	13	14	15	53
Estimated Outlays	*	8	13	14	15	50

* = between zero and $500,000.

The CBO staff contacts for this estimate are Matthew Pickford and Aldo Prosperi. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

* * * * * * *

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

* * * * * * *

SEC. 3607. DEFINITIONS

(a) IN GENERAL.—Except as provided under subsection (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) 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.

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

(3) FEDRAMP.—The term 'FedRAMP' means the Federal Risk and Authorization Management Program established under section 3608.

(4) 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 of General Services; or

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

(5) 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.

(6) FEDRAMP BOARD.—The term 'FedRAMP Board' means the board established under section 3610.

(7) INDEPENDENT ASSESSMENT ORGANIZATION.—The term 'independent assessment organization' means a third-party organization accredited by the Administrator of General Services to undertake conformity assessments of cloud service providers and their products or services.

(8) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

SEC. 3608. FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM

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

SEC. 3609. ROLES AND RESPONSIBILITIES OF THE GENERAL SERVICES ADMINISTRATION

(a) ROLES AND RESPONSIBILITIES.—The Administrator shall—

(1) in consultation with the Secretary, develop, coordinate, and implement a process to support agency review, reuse, and standardization, where appropriate, of security assessments of cloud computing products and services, including, as appropriate, 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 required 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 computing products and services that will receive a FedRAMP authorization, in consultation with the FedRAMP Board and the Chief Information Officers Council.

(c) EVALUATION OF AUTOMATION PROCEDURES.—

(1) IN GENERAL.—The Administrator, in coordination with the Secretary, shall assess and evaluate available automation

capabilities and procedures 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 security 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.

SEC. 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.

(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.

(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.

SEC. 3611. INDEPENDENCE 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.

SEC. 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.

SEC. 3613. ROLES AND RESPONSIBILITES 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 requirements beyond the security requirements included in a FedRAMP authorization for a particular control implementation.

SEC. 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 characteristics of cloud computing products and services that are within the scope of FedRAMP;

(B) includes requirements for agencies to obtain a FedRAMP authorization when operating a cloud computing product or service described in subparagraph (A) as a Federal information 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.

SEC. 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 following:

(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.

SEC. 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 consultation with the Director, 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 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 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 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 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 detailee 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.

○