The elimination of the so-called ''pre-funding mandate'' is a sensible first step towards improving the financial viability of the postal service. This bipartisan bill should also guide our approach to developing comprehensive postal reform legislation going forward. In stark contrast to the more partisan and sweeping reform proposals that have been presented to our committee in recent years, H.R. 2382 will immediately place the postal service on more sound financial footing while preserving its core public service mission to ''provide postal services to bind the nation together through the correspondence of the people.''

And contrary to the degradation of postal delivery services, or the wholesale privatization of the postal service itself, H.R. 2382 is the end product of bipartisan cooperation and the subject of broad consensus among our diverse postal stakeholders. As we develop additional postal reform legislation, it is imperative that we continue to identify fundamental and practical areas of agreement.

I urge my colleagues on both sides of the aisle to support this legislation.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Mrs. CAROLYN B. MALONEY) that the House suspend the rules and pass the bill, H.R. 2382.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Ms. FOXX of North Carolina. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, further proceedings on this motion will be postponed.

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM AUTHORIZATION ACT OF 2019

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 3941) to enhance the innovation, security, and availability of cloud computing services used in the Federal Government by establishing the Federal Risk and Authorization Management Program within the General Services Administration and by establishing a risk management, authorization, and continuous monitoring process to enable the Federal Government to leverage cloud computing services using a risk-based approach consistent with the Federal Information Security Modernization Act of 2014 and cloud-based operations, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 3941

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Federal Risk and Authorization Management Program Authorization Act of 2019'' or the ''FedRAMP Authorization Act''.

SEC. 2. CODIFICATION OF THE FEDRAMP PROGRAM.

(a) AMENDMENT.—Chapter 36 of title 44, United States Code, is amended by adding at the end the following new sections:

''§ 3607. Federal Risk and Authorization Management Program

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

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

''§ 3608. FedRAMP Program Management Office

''(a) GSA DUTIES.—

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

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

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

''(C) ensure the continuous improvement of FedRAMP.

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

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

''(B) hiring professional staff as may be necessary for the effective operation of the FedRAMP Program Management Office, and such other activities as are essential to properly perform critical functions;

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

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

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

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

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

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

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

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

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

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

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

''(c) EVALUATION OF AUTOMATION PROCEDURES.—

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

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

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

''§ 3609. Joint Authorization Board

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

''(1) The Department of Defense.

''(2) The Department of Homeland Security.

''(3) The General Services Administration.

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

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

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

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

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

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

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

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

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

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

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

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

''§ 3610. Independent assessment organizations

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

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

''§ 3611. Roles and responsibilities of agencies

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

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

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

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

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

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

''(b) SUBMISSION OF POLICIES REQUIRED.—Not later than 6 months after the date of the enactment of this section, the head of each agency shall submit to the Director the policies created pursuant to subsection (a)(1) for review and approval.

''(c) SUBMISSION OF AUTHORIZATIONS TO OPERATE REQUIRED.—Upon issuance of an authorization to operate or a provisional authorization to operate issued by an agency, the head of each agency shall provide a copy of the authorization to operate letter and any supplementary information required pursuant to section 3608(b) to the FedRAMP Program Management Office.

''(d) PRESUMPTION OF ADEQUACY.—

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

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

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

''The Director shall have the following duties:

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

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

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

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

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

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

''§ 3613. Authorization of appropriations for FEDRAMP

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

''§ 3614. Reports to Congress

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

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

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

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

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

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

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

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

''§ 3615. Federal Secure Cloud Advisory Committee

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

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

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

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

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

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

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

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

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

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

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

''(B) Submit reports as required.

''(b) MEMBERS.—

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

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

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

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

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

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

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

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

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

''(3) PERIOD OF APPOINTMENT; VACANCIES.—

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

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

''(c) MEETINGS AND RULES OF PROCEDURES.—

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

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

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

''(d) EMPLOYEE STATUS.—

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

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

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

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

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

''(h) INFORMATION FROM FEDERAL AGENCIES.—

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

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

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

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

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

''(l) REPORTS.—

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

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

''§ 3616. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

''(9) INDEPENDENT ASSESSMENT ORGANIZATION.—The term 'independent assessment organization' means a third-party organization accredited by the Program Director of the FedRAMP Program Management Office to undertake conformity assessments of cloud service providers.

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

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 36 of title 44, United States Code, is amended by adding at the end the following new items:

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

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

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

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from New York (Mrs. CAROLYN B. MALONEY) and the gentleman from North Carolina (Mr. MEADOWS) each will control 20 minutes.

The Chair recognizes the gentlewoman from New York.

GENERAL LEAVE

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on the measure before us.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from New York?

There was no objection.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I yield myself such time as I may consume.

I thank my colleagues and friends, Representatives CONNOLLY and MEADOWS, for their bipartisan work on this very important measure.

The Federal Risk and Authorization Management Program Authorization Act would codify and improve the existing FedRAMP program in the General Services Administration.

First established in 2011, FedRAMP is an important program that certifies cloud service providers that wish to offer services to the Federal Government. The FedRAMP certification process outlined in this bill is comprehensive and facilitates easier agency adoption, promotes agency reuse, and encourages savings.

The FedRAMP process uses a risk-based approach to ensure the reliability of any cloud platform that hosts unclassified government data. A significant provision of this bill is the Federal Secure Cloud Advisory Committee. This committee would be tasked with key responsibilities, including providing technical expertise on cloud products and services and identifying ways to reduce costs associated with FedRAMP certification.

The Director of the Office of Management and Budget would be required to issue regulations pertaining to FedRAMP and would ensure that agencies are not using cloud service providers without authorization.

This bill supports a critical effort to keep our Nation's information secure in cloud environments.

Mr. Speaker, I support this bill, and I reserve the balance of my time.

Mr. MEADOWS. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 3941, the FedRAMP Authorization Act.

Cybersecurity and IT modernization are both vital issues that we need to make sure run properly. The gentleman from Virginia (Mr. CONNOLLY) has been very proactive on this front.

The Federal Risk and Authorization Management Program, or FedRAMP, as it is commonly referred to, would allow Federal programs to focus on cybersecurity for cloud services, and it provides a process for agencies to follow when procuring cloud systems to ensure that those systems meet strict cybersecurity controls.

The gentlewoman, the chairman of the full committee, has certainly talked on a number of issues as it relates to this bill, but since there is no opposition that I am aware of, I will just submit my remarks for the RECORD.

Mr. Speaker, I rise in support of H.R. 3941, the FedRAMP Authorization Act.

Cyber security and IT modernization are both vital issues to ensure this government runs efficiently and effectively.

The Federal Risk and Authorization Management Program, or FedRAMP, is the main federal program focused on cyber security for cloud services.

It provides a process for agencies to follow when procuring cloud systems to ensure the systems meet strict cyber security controls.

Recent federal policies make the focus on securing cloud services especially important.

With the Cloud First initiative in 2011 and the Cloud Smart initiative from last year, the government has focused on implementation of cloud technologies.

The federal government has been plagued by reoccurring problems in information technology, such as low asset utilization, duplicative systems, and fragmented resources.

Shifting to the cloud provides for improved asset utilization, increased innovation, and a more responsive tech environment.

These improved efficiencies lead to a significant cost savings.

In fiscal year 2018, the government spent roughly six and a half billion dollars on cloud computing, with eighty four percent coming from FedRAMP authorized providers.

Efficiencies from FedRAMP saved agencies over two hundred fifty million dollars.

Codifying the program is an important step to encouraging agencies to take advantage of this program and all the benefits it offers.

I urge my colleagues to support the bill.

Mr. Speaker, I reserve the balance of my time.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I yield as much time as he may consume to the gentleman from Virginia (Mr. CONNOLLY), chair of the subcommittee.

Mr. CONNOLLY. Mr. Speaker, I thank the gentlewoman for yielding.

I salute my partner and friend on our subcommittee, Mr. MEADOWS. He chaired the subcommittee in the previous Congress, and I was his ranking member. We have reversed roles, but our partnership continues, especially in trying to modernize the Federal Government and bringing it into the 21st century in terms of information technology. We know that when we don't make those investments, bad things can happen. We just saw that the other night in the Iowa caucus.

H.R. 3941 codifies the Federal Risk and Authorization Management Program, known as FedRAMP, established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud computing technologies within the Federal Government.

FedRAMP standardizes security requirements for the authorization and ongoing cybersecurity assessments of cloud services for information systems across the Federal Government. In short, FedRAMP seeks to reduce the redundancies of Federal cloud migration and to help agencies quickly adopt cloud technologies.

I am also happy to say that FedRAMP has the approval of this administration. Last June, the Trump administration issued its Federal cloud computing strategy called Cloud Smart, which reaffirmed its support for FedRAMP. The Cloud Smart strategy acknowledged the importance of FedRAMP in helping agencies modernize their information technology systems.

Cloud Smart also highlighted improvements the program has implemented over the past few years that have resulted in a drastically reduced timeframe for providing a provisional authorization to operate a cloud service provider.

However, the administration also noted that there is still lack of reciprocity across agencies in taking advantage of FedRAMP-authorized products. Without that reciprocity, agencies end up duplicating the assessment process of cloud service offerings, leading to time delays and inefficiencies for both the Federal Government and the providers.

In July, the Subcommittee on Government Operations held a hearing to look at what the GSA has done right in administering the program and the ways in which FedRAMP can and should be improved. The message both from agency and industry witnesses was clear. FedRAMP is an important program that, if carried out effectively and efficiently, saves money for both agencies and businesses hoping to provide those services.

The FedRAMP Authorization Act codifies the program and addresses many of the concerns raised in July by both the administration and private-sector witnesses.

First, the bill reduces duplication of security assessments and other obstacles to agency adoption of cloud products by establishing—and this is really important—a presumption of adequacy for cloud technologies that have already received FedRAMP certification. Going to 33 different windows with 33 separate processes costs way too much money, takes way too much time, and, frankly, is unnecessary.

The presumption of adequacy means that the cloud service offering has met baseline security standards already established by the program and should be considered approved for use across the Federal Government, except where very specialized services would be required.

The bill also facilitates agency reuse of cloud technologies that have already received an authorization to operate by requiring agencies to check a centralized and secure repository and, to the extent practicable, reuse any existing security assessment before conducting an independent one of their own.

The desire to automate aspects of FedRAMP assessment processes was another key finding of the subcommittee's hearing. This bill requires the GSA work toward automating their processes, which will lead to more standard security assessments and continuous monitoring of cloud offerings to increase the efficiency for both providers and agencies.

The bill also establishes, as the distinguished chairwoman indicated, a Federal Secure Cloud Advisory Committee to ensure a dialogue among

GSA, agency cybersecurity and procurement officials, and industry in order to have effective and ongoing coordination in acquisition and adoption of cloud products by the Federal Government.

Finally, the bill authorizes the program at $20 million at an annual level, providing sufficient resources to increase the number of secure cloud technologies available for agency adoption.

We have worked with OMB, GSA, industry stakeholders, and our minority counterparts to ensure that this bill makes needed improvements in the FedRAMP program and gives the program the flexibility to grow and adopt to future changes in cloud technologies. I believe it is consistent with the administration's goals, and I urge adoption of the bill.

Mr. MEADOWS. Mr. Speaker, I yield myself the balance of my time.

I thank the gentleman for his leadership on this. I will say that I have had a number of conversations in recent weeks with stakeholders who have offered some suggestions on what we could do, so I look forward to working with the gentleman opposite on how we can address this critical issue.

Mr. Speaker, I would urge support and adoption of this measure, and I yield back the balance of my time.

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I yield myself the balance of my time.

I urge passage of H.R. 3941, as amended, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from New York (Mrs. CAROLYN B. MALONEY) that the House suspend the rules and pass the bill, H.R. 3941, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

PAYMENT INTEGRITY INFORMATION ACT OF 2019

Mrs. CAROLYN B. MALONEY of New York. Mr. Speaker, I move to suspend the rules and pass the bill (S. 375) to improve efforts to identify and reduce Governmentwide improper payments, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 375

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 ''Payment Integrity Information Act of 2019''.

SEC. 2. IMPROPER PAYMENTS.

(a) IN GENERAL.—Chapter 33 of title 31, United States Code, is amended by adding at the end the following:

''Subchapter IV—Improper Payments

''§ 3351. Definitions

''In this subchapter:

''(1) ANNUAL FINANCIAL STATEMENT.—The term 'annual financial statement' means the annual financial statement required under section 3515 of this title or similar provision of law.

''(2) COMPLIANCE.—The term 'compliance' means that an executive agency—

''(A) has—

''(i) published improper payments information with the annual financial statement of the executive agency for the most recent fiscal year; and

''(ii) posted on the website of the executive agency that statement and any accompanying materials required under guidance of the Office of Management and Budget;

''(B) if required, has conducted a program specific risk assessment for each program or activity that conforms with the requirements under section 3352(a);

''(C) if required, publishes improper payments estimates for all programs and activities identified under section 3352(a) in the accompanying materials to the annual financial statement;

''(D) publishes programmatic corrective action plans prepared under section 3352(d) that the executive agency may have in the accompanying materials to the annual financial statement;

''(E) publishes improper payments reduction targets established under section 3352(d) that the executive agency may have in the accompanying materials to the annual financial statement for each program or activity assessed to be at risk, and has demonstrated improvements and developed a plan to meet the reduction targets; and

''(F) has reported an improper payment rate of less than 10 percent for each program and activity for which an estimate was published under section 3352(c).

''(3) DO NOT PAY INITIATIVE.—The term 'Do Not Pay Initiative' means the initiative described in section 3354(b).

''(4) IMPROPER PAYMENT.—The term 'improper payment'—

''(A) means any payment that should not have been made or that was made in an incorrect amount, including an overpayment or underpayment, under a statutory, contractual, administrative, or other legally applicable requirement; and

''(B) includes—

''(i) any payment to an ineligible recipient;

''(ii) any payment for an ineligible good or service;

''(iii) any duplicate payment;

''(iv) any payment for a good or service not received, except for those payments where authorized by law; and

''(v) any payment that does not account for credit for applicable discounts.

''(5) PAYMENT.—The term 'payment' means any transfer or commitment for future transfer of Federal funds such as cash, securities, loans, loan guarantees, and insurance subsidies to any non-Federal person or entity or a Federal employee, that is made by a Federal agency, a Federal contractor, a Federal grantee, or a governmental or other organization administering a Federal program or activity.

''(6) PAYMENT FOR AN INELIGIBLE GOOD OR SERVICE.—The term 'payment for an ineligible good or service' includes a payment for any good or service that is rejected under any provision of any contract, grant, lease, cooperative agreement, or other funding mechanism.

''(7) RECOVERY AUDIT.—The term 'recovery audit' means a recovery audit described in section 3352(i).

''(8) STATE.—The term 'State' means each State of the United States, the District of Columbia, each territory or possession of the United States, and each Federally recognized Indian tribe.

''§ 3352. Estimates of improper payments and reports on actions to reduce improper payments

''(a) IDENTIFICATION OF SUSCEPTIBLE PROGRAMS AND ACTIVITIES.—

''(1) IN GENERAL.—The head of each executive agency shall, in accordance with guidance prescribed by the Director of the Office of Management and Budget—

''(A) periodically review all programs and activities that the head of the executive agency administers; and

''(B) identify all programs and activities with outlays exceeding the statutory threshold dollar amount described in paragraph (3)(A)(i) that may be susceptible to significant improper payments.

''(2) FREQUENCY.—A review under paragraph (1) shall be performed for each program and activity that the head of an executive agency administers not less frequently than once every 3 fiscal years.

''(3) RISK ASSESSMENTS.—

''(A) DEFINITION OF SIGNIFICANT.—In this paragraph, the term 'significant' means that, in the preceding fiscal year, the sum of a program or activity's improper payments and payments whose propriety cannot be determined by the executive agency due to lacking or insufficient documentation may have exceeded—

''(i) $10,000,000 of all reported program or activity payments of the executive agency made during that fiscal year and 1.5 percent of program outlays; or

''(ii) $100,000,000.

''(B) SCOPE.—In conducting a review under paragraph (1), the head of each executive agency shall take into account those risk factors that are likely to contribute to a susceptibility to significant improper payments, such as—

''(i) whether the program or activity reviewed is new to the executive agency;

''(ii) the complexity of the program or activity reviewed;

''(iii) the volume of payments made through the program or activity reviewed;

''(iv) whether payments or payment eligibility decisions are made outside of the executive agency, such as by a State or local government;

''(v) recent major changes in program funding, authorities, practices, or procedures;

''(vi) the level, experience, and quality of training for personnel responsible for making program eligibility determinations or certifying that payments are accurate;

''(vii) significant deficiencies in the audit report of the executive agency or other relevant management findings that might hinder accurate payment certification;

''(viii) similarities to other programs or activities that have reported improper payment estimates or been deemed susceptible to significant improper payments;

''(ix) the accuracy and reliability of improper payment estimates previously reported for the program or activity, or other indicator of potential susceptibility to improper payments identified by the Inspector General of the executive agency, the Government Accountability Office, other audits performed by or on behalf of the Federal, State, or local government, disclosures by the executive agency, or any other means;

''(x) whether the program or activity lacks information or data systems to confirm eligibility or provide for other payment integrity needs; and

''(xi) the risk of fraud as assessed by the executive agency under the Standards for Internal Control in the Federal Government published by the Government Accountability Office (commonly known as the 'Green Book').