

115TH CONGRESS
2D SESSION

H. R. 6550

To enhance the innovation, security, and availability of Federal Government cloud services by establishing the Federal Risk and Authorization Management Program within the Office of Management and Budget Office of Electronic Government 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 Reform Act of 2014 and cloud-based operations, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 26, 2018

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

A BILL

To enhance the innovation, security, and availability of Federal Government cloud services by establishing the Federal Risk and Authorization Management Program within the Office of Management and Budget Office of Electronic Government 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 Reform Act of 2014 and cloud-based operations, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Risk and Au-
5 thorization Management Program Reform Act of 2018”
6 or the “FedRAMP Authorization Act”.

7 **SEC. 2. CODIFICATION OF THE FEDRAMP PROGRAM.**

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

11 **“§ 3607. Federal Risk and Authorization Management**
12 **Program**

13 “(a) ESTABLISHMENT.—There is established within
14 the General Services Administration, an office to be known
15 as the FedRAMP Program Management Office that shall
16 be responsible for the Federal Risk and Authorization
17 Management Program. FedRAMP is a specific Govern-
18 ment certification program that examines and accredits
19 cloud service providers that offer Federal cloud computing
20 services for sale, lease, or purchase to Federal agency
21 cloud customers. The FedRAMP Program Management
22 Office embodies the goal of a ‘qualify once, use many
23 times’ process through the issuance of certifications in the
24 form of provisional authorizations to operate.

1 “(b) COMPONENTS OF FEDRAMP.—There are estab-
2 lished as components of FedRAMP the Joint Authoriza-
3 tion Board and the Program Management Office, or such
4 successor offices as the Office of Management and Budg-
5 et, through the Office of Electronic Government may de-
6 termine.

7 “(c) FEDRAMP DUTIES.—The Director of the Office
8 of Management and Budget and the Administrator of
9 General Services, or their designees, shall work together
10 to do the following:

11 “(1) Issue guidance on categories and charac-
12 teristics of information technology goods or services
13 that are within the jurisdiction of FedRAMP and
14 that require FedRAMP certification.

15 “(2) Issue guidance for the establishment and
16 implementation of FedRAMP to conduct security as-
17 sessments, reviews, and appropriate oversight of con-
18 tinuous monitoring of cloud services used by agen-
19 cies.

20 “(3) Not later than 180 days after the date of
21 the enactment of this section, and annually there-
22 after, submit to Congress a report on the status and
23 performance of the FedRAMP Program Manage-
24 ment Office, including the status and disposition of
25 waiver requests to FedRAMP submitted to the

1 FedRAMP Program Management Office by agencies
2 and a description of and progress towards meeting
3 the metrics adopted by the FedRAMP Program
4 Management Office pursuant to section 3608(e), as
5 submitted to the Administrator by that Office.

6 **“§ 3608. Roles and responsibilities of the FedRAMP**
7 **Program Management Office**

8 “(a) IMPLEMENTATION.—Upon delegation from the
9 Office of Electronic Government, the Administrator shall
10 oversee the implementation of FedRAMP, including—

11 “(1) appointing a Program Director to oversee
12 the FedRAMP Program Management Office;

13 “(2) hiring professional staff as may be nec-
14 essary for the effective operation of the FedRAMP
15 Program Management Office, and such other activi-
16 ties as are essential to properly perform critical
17 functions; and

18 “(3) such other actions as the Administrator
19 may determine necessary to carry out this section.

20 “(b) AUTHORITY AND DUTIES.—The FedRAMP Pro-
21 gram Management Office shall have the following author-
22 ity and duties:

23 “(1) Provide guidance to agencies, regarding
24 compliance with requirements, guidelines, and stand-

1 ards developed by the National Institute of Stand-
2 ards and Technology.

3 “(2) Provide guidance to third party assess-
4 ment organizations in using and applying the re-
5 quirements, guidelines, and standards adopted by
6 FedRAMP.

7 “(3) Provide guidance to agencies on appro-
8 priate use of and acquisition of FedRAMP approved
9 services, including the role of cloud brokers and
10 cloud service integrators.

11 “(4) In consultation with the Director and the
12 Secretary of Homeland Security, issue guidance for
13 agencies on monitoring and reporting on the usage
14 and demand of cloud computing, use of automation,
15 and use of commercial cloud services to the fullest
16 extent practical.

17 “(5) In consultation with the Federal Chief In-
18 formation Officer, oversee and issue guidelines re-
19 garding the qualifications, roles, and responsibilities
20 of third party assessment organizations, in consulta-
21 tion with the National Institute of Standards and
22 Technology.

23 “(6) Develop standards and templates, includ-
24 ing a summary risk report template for third party
25 assessment organizations that informs the security

1 assessment report to complement the existing au-
2 thorization package artifacts and serve as an author-
3 ization decision-making tool.

4 “(7) Coordinate with stakeholders to provide
5 guidance and recommendations to FedRAMP.
6 Stakeholders to include—

7 “(A) agency cloud customers;

8 “(B) cloud service providers;

9 “(C) third party assessment organizations;

10 “(D) agency Offices of Inspector General;

11 and

12 “(E) the Government Accountability Of-
13 fice.

14 “(8) Establish and maintain a public comment
15 process for newly issued or revised guidance adopted
16 by FedRAMP.

17 “(c) EVALUATION OF AUTOMATION PROCEDURES.—
18 The FedRAMP Program Management Office shall assess
19 and evaluate available automation procedures to accelerate
20 the processing of FedRAMP applications.

21 “(d) METRICS FOR CERTIFICATION.—The FedRAMP
22 Program Management Office shall adopt specific metrics
23 regarding the time, cost, and quality of the assessments
24 necessary for completion of a FedRAMP authorization
25 process in a manner that can be consistently tracked over

1 time, which shall be done in conjunction with the periodic
2 testing and evaluation process pursuant to subchapter II
3 of chapter 35 in a manner that minimizes the agency re-
4 porting burden.

5 **“§ 3609. Roles and responsibilities of the Joint Au-**
6 **thorization Board**

7 “(a) ESTABLISHMENT.—There is established the
8 Joint Authorization Board which shall consist of the Chief
9 Information Officers or their designees of the Department
10 of Defense, the Department of Homeland Security, and
11 the General Services Administration.

12 “(b) ISSUANCE OF PROVISIONAL AUTHORIZATIONS
13 TO OPERATE.—The Joint Authorization Board shall have
14 the authority to issue provisional authorizations to operate
15 to cloud service providers that meet FedRAMP security
16 guidelines set forth in the Common Security Control Base-
17 line.

18 “(c) DUTIES.—The Joint Authorization Board
19 shall—

20 “(1) review and validate cloud service provider
21 and third party assessment organization security as-
22 sessment packages;

23 “(2) in consultation with the FedRAMP Pro-
24 gram Management Office, serve as a resource for
25 best practices to accelerate the FedRAMP process;

1 “(3) obtain such professional staff as may be
2 necessary for the effective operation of FedRAMP
3 and such other activities as are essential to properly
4 perform critical functions;

5 “(4) such other roles and responsibilities as the
6 FedRAMP Program Management Office may assign,
7 as agreed to by the FedRAMP Program Manage-
8 ment Office and members of the Joint Authorization
9 Board; and

10 “(5) appoint technical representatives respon-
11 sible for FedRAMP activities within each Joint Au-
12 thorization Board agency.

13 **“§ 3610. Roles and responsibilities of third party as-**
14 **essment organizations**

15 “(a) REQUIREMENTS FOR CERTIFICATION.—The
16 FedRAMP Program Management Office, in consultation
17 with the Joint Authorization Board, shall determine the
18 requirements for certification of third party assessment
19 organizations. Such requirements may include developing
20 or requiring certification programs for individuals em-
21 ployed by the third party assessment organizations who
22 lead FedRAMP assessment teams.

23 “(b) ASSESSMENT.—Accredited third party assess-
24 ment organizations shall assess, validate, and attest to the

1 quality and compliance of security assessment materials
2 provided by cloud service providers.

3 “(c) SUMMARY RISK REPORT.—Accredited third
4 party assessment organizations shall develop a risk report
5 that summarizes the security assessment report to com-
6 plement the existing authorization package artifacts and
7 serve as an authorization decision making tool.

8 **“§ 3611. Roles and responsibilities of agencies**

9 “(a) IN GENERAL.—In implementing and enforcing
10 the requirements of FedRAMP, Federal agency cloud cus-
11 tomers shall—

12 “(1) create policies to implement FedRAMP re-
13 quirements;

14 “(2) issue agency-specific authorizations to op-
15 erate for Federal cloud computing services in com-
16 pliance with subchapter II of chapter 35;

17 “(3) be in compliance with any FedRAMP re-
18 quirements, unless a waiver is issued by the Direc-
19 tor;

20 “(4) provide data to the Director on how agen-
21 cies are meeting metrics as defined by the
22 FedRAMP Program Management Office pursuant to
23 section 3614(b); and

24 “(5) if applicable, ensure that any contract is in
25 compliance with FedRAMP requirements.

1 “(b) SUBMISSION OF POLICIES REQUIRED.—Not
2 later than 6 months after the date of the enactment of
3 this section, Federal agency cloud customers shall submit
4 to the Director the policies created pursuant to subsection
5 (a)(1) for review and approval.

6 “(c) SUBMISSION OF AUTHORIZATIONS TO OPERATE
7 REQUIRED.—Upon issuance of an authorization to oper-
8 ate, the head of the relevant agency shall provide a copy
9 of the authorization to operate letter to the FedRAMP
10 Program Management Office and the cloud service pro-
11 vider to enable the FedRAMP Program Management Of-
12 fice to track and assess all forms of authorizations to oper-
13 ate on a Governmentwide basis.

14 “(d) PRESUMPTION OF ADEQUACY.—Any provisional
15 authorization to operate issued by the Joint Authorization
16 Board shall be considered to be presumptively adequate
17 by agencies, subject to technical or programmatic rebuttal
18 by an agency that disagrees with adequacy or sufficiency
19 of the certification. This rebuttable presumption of ade-
20 quacy shall not derogate, modify, or alter the responsi-
21 bility of any agency to ensure compliance with the sub-
22 chapter II of chapter 35 for any Federal cloud computing
23 services that the agency deploys.

24 “(e) WAIVER OR EXCEPTION.—The Chief Informa-
25 tion Officer of each agency may request a waiver or excep-

1 tion to specific FedRAMP requirements. Such request for
2 waiver shall be in accordance with the determinations and
3 finding issued under section 3612(2). The determination
4 and findings shall be submitted to the FedRAMP Program
5 Management Office and the Director, along with such sup-
6 porting articles as may be required under guidelines issued
7 by FedRAMP.

8 “(f) AGENCY REPORTS REQUIRED.—Not later than
9 90 days after the date of which any guidance is issued
10 pursuant to section 3608(b)(4) from the FedRAMP Pro-
11 gram Management Office, the head of each agency shall
12 submit to the Director a report on cloud computing usage
13 and the potential demand for cloud computing.

14 **“§ 3612. Roles and Responsibilities of the Office of**
15 **Management and Budget**

16 “The Director shall have the following duties:

17 “(1) Highlight current guidance or issue new
18 guidance to ensure that an agency does not operate
19 a Federal Government cloud computing service using
20 Government data without issuing an authorization to
21 operate issued by the agency that meets the require-
22 ments of subchapter II of chapter 35 and
23 FedRAMP.

24 “(2) Issue guidance and templates for agency
25 determinations and findings for waivers to the re-

1 requirements of FedRAMP (any request by an agency
2 for such a waiver must set forth unique agency-spe-
3 cific technical, operational, or managerial require-
4 ments necessary for agency operations).

5 “(3) Define alternatives and agency best prac-
6 tices for compliance with the Trusted Internet Con-
7 nection for agencies connecting to a cloud service
8 provider.

9 “(4) Grant waivers or exceptions to specific
10 FedRAMP requirements as may be necessary by the
11 submission of agency determinations and findings
12 that meet the OMB guidelines for FedRAMP waiv-
13 ers pursuant to paragraph (2).

14 “(5) Ensure agencies are in compliance with
15 any guidance or other requirements issued related to
16 FedRAMP.

17 **“§ 3613. Funding of FedRAMP**

18 “The FedRAMP Program Management Office may,
19 to the extent deemed appropriate by the Administrator
20 and in consultation with the Director, use funds contained
21 within the Acquisition Services Fund described under sec-
22 tion 321 of title 40 or such other funds as may be avail-
23 able for the operations of FedRAMP.

1 **“§ 3614. Reporting**

2 “(a) IN GENERAL.—Not later than 18 months after
3 the date of the enactment of this section, and annually
4 thereafter, the Director shall submit to the Committee on
5 Oversight and Government Reform of the House of Rep-
6 resentatives and the Committee on Homeland Security
7 and Government Affairs of the Senate a report that in-
8 cludes the following:

9 “(1) The status, efficiency, and effectiveness of
10 FedRAMP during the preceding year in authorizing
11 and recertifying secure cloud solutions for Federal
12 agency cloud customers.

13 “(2) The length of time for Federal agency
14 cloud customers to issue authorizations to operate
15 during the preceding year.

16 “(3) Agency requests for FedRAMP waivers.

17 “(4) Progress during the preceding year in ad-
18 vancing automation techniques to securely automate
19 FedRAMP processes and to accelerate reporting as
20 described in this section.

21 “(5) Number of cloud computing systems in use
22 at each agency and the number of cloud computing
23 authorizations to operate.

24 “(b) GAO REPORT.—Not later than 2 years after the
25 date of enactment of this section, and every three years
26 thereafter, the Comptroller General shall submit to the

1 Oversight and Government Reform Committee of the
2 House of Representatives and the Homeland Security and
3 Governmental Affairs Committee of the Senate an assess-
4 ment of FedRAMP, third party assessment organizations,
5 and Federal agency cloud customers, including the fol-
6 lowing:

7 “(1) An evaluation of the impact and con-
8 tinuing need for specific cloud security controls.

9 “(2) A review of the adequacy of resources to
10 run FedRAMP.

11 “(3) The development of reusability and the po-
12 tential for the use and adoption of reciprocal stand-
13 ards, whether from Government or the private sec-
14 tor, as substitutes for specific security controls in
15 use by the FedRAMP Project Management Office.

16 **“§ 3615. Definitions**

17 “(a) IN GENERAL.—Except as provided under para-
18 graph (2), the definitions under sections 3502 and 3552
19 apply to sections 3607 through 3614.

20 “(b) ADDITIONAL DEFINITIONS.—In sections 3607
21 through 3614:

22 “(1) ADMINISTRATOR.—The term ‘Adminis-
23 trator’ means the Administrator of General Services.

24 “(2) CLOUD BROKER.—The term ‘cloud broker’
25 means an entity that manages the use, performance,

1 and delivery of cloud computing services and nego-
2 tiates relationships between cloud service providers
3 and cloud consumers.

4 “(3) CLOUD COMPUTING.—The term ‘cloud
5 computing’ means a model for enabling ubiquitous,
6 convenient, on-demand network access to a shared
7 pool of configurable computing resources (such as
8 networks, servers, storage, applications, and serv-
9 ices) that can be rapidly provisioned and released
10 with minimal management effort or service provider
11 interaction (as defined by the National Institute of
12 Standards and Technology pursuant to the National
13 Institute of Standards and Technology Act (15
14 U.S.C. 278g–3), including NIST Special Publication
15 800–145) or any successor thereto.

16 “(4) CLOUD SERVICE INTEGRATOR.—The term
17 ‘cloud service integrator’ means a systems or service
18 integrator that specializes in cloud computing serv-
19 ices.

20 “(5) CLOUD SERVICE PROVIDER.—The term
21 ‘cloud service provider’ means a third party entity
22 offering cloud computing services to the Federal
23 Government.

1 “(6) COMMON SECURITY CONTROL BASELINE.—

2 The term ‘common security control baseline’ means
3 the guidance issued pursuant to section 3607(c)(2).

4 “(7) DIRECTOR.—The term ‘Director’ means
5 the Director of the Office of Management and Budget.
6 et.

7 “(8) FEDERAL AGENCY CLOUD CUSTOMER.—

8 The term ‘Federal agency cloud customer’ means an
9 agency using cloud computing services.

10 “(9) FEDERALLY CONTROLLED INFORMATION

11 SYSTEM.—The term ‘federally controlled information
12 system’ or ‘Federal information system’ means an
13 information system used or operated by a Federal
14 agency cloud customer as set forth and in compli-
15 ance with the guidelines and requirements of section
16 3554 of title 40.

17 “(10) FEDERAL GOVERNMENT CLOUD COM-

18 PUTING SERVICES.—The term ‘Federal Government
19 cloud computing services’ means a cloud computing
20 service that is used or operated by a Federal agency
21 cloud customer upon a federally controlled informa-
22 tion system.

23 “(11) FEDRAMP.—The term ‘FedRAMP’

24 means the Federal Risk and Authorization Manage-
25 ment Program established under section 3607(a).

1 “(12) FEDRAMP PROGRAM MANAGEMENT OF-
2 FICE.—The term ‘FedRAMP Program Management
3 Office’ means the office that administers FedRAMP.

4 “(13) FEDRAMP SECURITY CONTROLS BASE-
5 LINE.—The term ‘FedRAMP security controls base-
6 line’ means those security controls that cloud service
7 providers and agencies must, at a minimum, address
8 to receive a provisional authorization to operate, as
9 defined by the FedRAMP Program Management Of-
10 fice.

11 “(14) JOINT AUTHORIZATION BOARD.—The
12 term ‘Joint Authorization Board’ means the Joint
13 Authorization Board established under section 3609.

14 “(15) TECHNICAL REPRESENTATIVE.—The
15 term ‘technical representative’ means an agency’s
16 technical representative to the Joint Authorization
17 Board designated by the member agency of the
18 Joint Authorization Board.

19 “(16) THIRD PARTY ASSESSMENT ORGANIZA-
20 TION.—The term ‘third party assessment organiza-
21 tion’ means a third-party organization accredited by
22 the Program Director of the FedRAMP Program
23 Management Office to undertake conformity assess-
24 ments of cloud service providers.”.

1 (b) TECHNICAL AND CONFORMING AMENDMENT.—

2 The table of sections for chapter 36 of title 44, United

3 States Code, is amended by adding at the end the fol-

4 lowing new items:

“3607. Federal Risk and Authorization Management Program.

“3608. Roles and responsibilities of the FedRAMP Program Management
Office.

“3609. Roles and responsibilities of the Joint Authorization Board.

“3610. Roles and responsibilities of third party assessment organizations.

“3611. Roles and responsibilities of the agencies.

“3612. Funding of FedRAMP.

“3613. Reporting.

“3614. Definitions.”.

