AMENDMENT TO RULES COMMITTEE PRINT 117–13

OFFERED BY MR. CONNOLLY OF VIRGINIA

Page 1390, after line 19, add the following new section (and update the table of contents accordingly):

SEC. 6013. 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

There is established within the General Services Administration the Federal Risk and Authorization Management Program (FedRAMP). The Administrator of General Services, subject to section 3612, shall establish a governmentwide 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.

“§ 3608. Roles and responsibilities of the general services administration

(a) ROLES AND RESPONSIBILITIES.—The Administrator of General Services shall—
“(1) 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 appropriate oversight of continuous monitoring of cloud computing products and services, pursuant to guidance issued by the Director pursuant to section 3612;

“(2) establish processes and identify criteria, consistent with guidance issued by the Director in section 3612, which would 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 defined by the National Institute of Standards and Technology and relevant statutes;

“(4) grant FedRAMP authorizations to cloud computing products and services, consistent with the
guidance and direction of the FedRAMP board established in section 3609;

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

“(6) 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, to establish and regularly update a framework for continuous monitoring under section 3553;

“(7) 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 subsection 3611;

“(8) provide regular updates to applicant cloud service providers on the status of any cloud computing product or service during an assessment process;
“(9) regularly review, in consultation with the FedRAMP Board, the costs associated with the independent assessment services of third-party organizations referenced in section 3610;

“(10) support the Federal Secure Cloud Advisory Committee, established pursuant to subsection 3615; and

“(11) such other actions as the Administrator may determine necessary to improve the program.

“(b) WEBSITE.—

“(1) IN GENERAL.—The Administrator shall maintain a public website to serve as the authoritative repository for the program, 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 established in section 3603.
“(c) Evaluation of Automation Procedures.—

“(1) In General.—The Administrator 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 the 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.

§ 3609. FedRAMP board

“(a) Establishment.—There is established a FedRAMP board to provide input and recommendations to the Administrator regarding the requirements and guidelines for security assessments of cloud computing
products and services developed under subsection (d) of this section.

“(b) **MEMBERSHIP.**—The board shall consist of not more than seven senior officials or experts from agencies, appointed by the Director, in consultation with the Administrator, from each of the following:

“(1) The Department of Defense.


“(3) The General Services Administration.

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

“(c) **QUALIFICATIONS.**—Members of the FedRAMP board appointed under subsection (b) shall have technical expertise in domains relevant to the program, 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) review and approve requirements and guidelines for security authorizations of cloud computing products and services, consistent with standards defined by 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 3611(b), and ensure consistency and transparency between agencies and cloud service providers in a manner that minimizes confusion and engenders trust; and

“(4) 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 established in section 3603 to establish a process, that may be made available the website referenced in section 3608, for prioritizing and accepting the cloud com-
puting products and services to be granted a FedRAMP authorization.

“§ 3610. Independent assessment organizations

“(a) REQUIREMENTS FOR ACCREDITATION.—The Administrator may, consistent with guidance issued by the Director, determine the requirements for accreditation of a third-party organization to perform independent assessments and other activities that will improve the overall performance of the program and reduce the cost of FedRAMP authorizations for cloud service providers. Such requirements may include developing or requiring certification programs for individuals employed by the third-party organization seeking accreditation.

“(b) CERTIFICATION.—The Administrator or their designee may accredit any third-party organization that meets the requirements for accreditation. If accredited pursuant to the requirements defined pursuant to subsection (a), a certified independent assessment organization 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 the program, the head of each agency shall, con-
consistent with guidance issued by the Director pursuant to
section 3612—

“(1) promote the use of cloud computing prod-
ucts and services which meet FedRAMP security re-
quirements and other risk-based performance re-
quirements as defined by the Director;

“(2) confirm whether there is a FedRAMP au-
thorization in the secure mechanism established
under section 3608(b)(10) before beginning the
process to grant 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 au-
thorize that has received a FedRAMP authorization,
use the existing assessments of security controls and
materials within the FedRAMP authorization pack-
age; and

“(4) provide data and information required to
the Director pursuant to section 3612 to determine
how agencies are meeting metrics as defined by the
Administrator.

“(b) ATTESTATION.—To the extent an agency deter-
mines that the information and data they have reviewed
pursuant to subsection (a)(2) is wholly or substantially de-
ficient for the purposes of performing an authorization of
cloud computing products or services, the head of the agency shall document as part of the resulting FedRAMP authorization package the reasons for this determination upon completion of any assessment or authorization activities for that particular cloud computing product or service.

“(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 3608(a) to the Administrator.

“(d) Submission of Policies Required.—Not later than 6 months after the date on which the Director issues guidance in accordance with section 3612, the head of each agency, acting through the agency Chief Information Officer, shall submit to the Director all agency policies created related 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 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

“(a) ROLES AND RESPONSIBILITIES.—The Director shall:

“(1) Issue guidance to specify the categories or characteristics of cloud computing products and services, in consultation with the Administrator, for which agencies must obtain or use a FedRAMP authorization before operating such a product or service as a Federal information system. Such guidance shall encompass, to the greatest extent practicable, all necessary and appropriate cloud computing products and services.

“(2) Issue guidance describing additional responsibilities of the FedRAMP program and board to accelerate the adoption of secure cloud computing services in the Federal Government.

“(3) Oversee the effectiveness of the FedRAMP program and board, including compliance by the
FedRAMP board with its duties as described in section 3609.

“(4) To the greatest extent practicable, encourage and promote consistency of guidance on the adoption, security, and use of cloud computing products and services used within agencies.

“§ 3613. Authorization of appropriations for FedRAMP

“There is authorized to be appropriated $20,000,000 each year for the FedRAMP Program and Board.

“§ 3614. Reports to congress; GAO report

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

“(1) The status, efficiency, and effectiveness of the General Services Administration, pursuant to section 3608, and agencies, pursuant to section 3611, during the preceding year in supporting the speed, effectiveness, sharing, reuse, and security of authorizations to operate for cloud computing products and services.
“(2) Progress towards meeting the metrics required pursuant to section 3608(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 previous year.

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

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

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

§ 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 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 services offered by small businesses (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 are, at a minimum, to provide advice and recommendations to the Administrator, the FedRAMP Board, and to agencies on technical, financial, programmatic, and operational matters regarding secure adoption of cloud computing products and services.

“(b) MEMBERS.—

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

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

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

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

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

“(E) At least one individual representing an independent assessment organization.

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

“(G) At least two other Government representatives as the Administrator determines to be necessary to provide sufficient balance, insights, or expertise to the Committee.
“(2) **Deadline for Appointment.**—Each member of the Committee shall be appointed not later than 90 days after the date of the enactment of this section.

“(3) **Period of Appointment; Vacancies.**—

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

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

“(c) **Meetings and Rules of Procedures.**—
“(1) MEETINGS.—The Committee shall hold not fewer than three meetings in a calendar year, at such time and place as determined by the Chair.

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

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

“(d) EMPLOYEE STATUS.—

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

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

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

“(f) 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 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) CLOUD COMPUTING.—The term ‘cloud computing’ shall have the meaning given by the National Institutes of Standards and Technology Special Publication 800–145.

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

(4) DIRECTOR.—The term ‘Director’ means the Director of the Office of Management and Budget.


(6) FEDRAMP AUTHORIZATION.—The term ‘FedRAMP authorization’ means a certification that a cloud computing product or service has completed a FedRAMP authorization process, as determined by the Administrator or received a FedRAMP provi-
sional authorization to operate as determined by the
FedRAMP Board.

“(7) 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 the FedRAMP program.

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

“(9) FedRAMP BOARD.—The term ‘FedRAMP board’ means the 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. Roles and Responsibilities of the General Services Administration
‘3609. FedRAMP board
‘3610. Independent assessment organizations
‘3611. Roles and responsibilities of agencies
22

‘‘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’’.

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

(d) RULE OF CONSTRUCTION.—Nothing in this sec-
tion or any amendment made by this section shall be con-
strued as altering or impairing the authorities of the Di-
rector of the Office of Management and Budget or the
Secretary of Homeland Security under subchapter II of
chapter 35 of title 44, United States Code.