116TH CONGRESS
2D SESSION

S. 4785

To require the Director of the Office of Management and Budget to develop a model for risk-based budgeting, and for other purposes.

IN THE SENATE OF THE UNITED STATES

OCTOBER 1, 2020

Mr. PORTMAN (for himself and Mr. PETERS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To require the Director of the Office of Management and Budget to develop a model for risk-based budgeting, and for other purposes.

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 ''Risk-Informed Spending for Cybersecurity Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

(B) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ''covered agency'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code.

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

(4) INFORMATION TECHNOLOGY.—The term ''information technology''—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

(B) includes the hardware and software systems of a Federal agency that monitor and control physical equipment and processes of the Federal agency.

(5) RISK-BASED BUDGET.—The term ''risk-based budget'' means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

SEC. 3. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) IN GENERAL.—

(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with the Director of the National Institute of Standards and Technology, shall develop a standard model for creating a risk-based budget for cybersecurity spending.

(2) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, is amended—

(A) in paragraph (5), by striking ''and'' at the end;

(B) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(7) developing a standard risk-based budget model to inform Federal agency cybersecurity budget development.''.

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—

(A) consider Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(B) consider the impact of agency operations of compromise of systems, including the interconnectivity to other agency systems and the operations of other agencies;

(C) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;

(D) be used to inform acquisition and sustainment of—

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

(iv) cybersecurity and information technology concepts of operations; and

(E) be used to evaluate and inform government-wide cybersecurity programs of the Department of Homeland Security.

(4) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under this subsection.

(5) PUBLICATION.—The Director shall publish the model required to be developed under this subsection, and any updates necessary under paragraph (4), on the public website of the Office of Management and Budget.

(6) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until

the date on which the model required to be developed under this subsection is completed, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

(b) REQUIRED USE OF RISK-BASED BUDGET MODEL.—

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

(2) AGENCY PERFORMANCE PLANS.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ''and the risk-based budget model required under section 3553(a)(7)'' after ''paragraph (1)''.

(c) VERIFICATION.—

(1) IN GENERAL.—Section 1105(a)(35)(A)(i) of title 31, United States Code, is amended—

(A) in the matter preceding subclause (I), by striking ''by agency, and by initiative area (as determined by the administration)'' and inserting ''and by agency'';

(B) in subclause (III), by striking ''and'' at the end;

(C) in subclause (IV), by adding ''and'' at the end; and

(D) by adding at the end the following:

''(V) a validation that the budgets submitted were developed using a risk-based methodology;''.

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) ANNUAL REPORTS.—

(1) ANNUAL INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

(A) in subparagraph (B), by striking ''and'' at the end;

(B) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(D) an assessment of how the agency implemented the risk-based budget model required under section 3553(a)(7) and an evaluation of

whether the model mitigates agency cyber vulnerabilities.''.

(2) ASSESSMENT.—Section 3553(c) of title 44, United States Code, is amended—

(A) in paragraph (4), by striking ''and'' at the end;

(B) in paragraph (5), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(6) an assessment of—

''(A) Federal agency implementation of the model required under subsection (a)(7);

''(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

''(C) whether the model mitigates the cyber vulnerabilities of the Federal Government.''.

(e) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by subsection (c), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

(2) an evaluation of the success of covered agencies in implementing risk-based budgets;

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerability, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

(4) any other information relating to risk-based budgets the Comptroller General determines appropriate.

○