

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.

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 “Risk-Informed Spend-
5 ing for Cybersecurity Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) APPROPRIATE CONGRESSIONAL COMMIT-
2 TEES.—The term “appropriate congressional com-
3 mittees” means—

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

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

10 (2) COVERED AGENCY.—The term “covered
11 agency” has the meaning given the term “executive
12 agency” in section 133 of title 41, United States
13 Code.

14 (3) DIRECTOR.—The term “Director” means
15 the Director of the Office of Management and Budg-
16 et.

17 (4) INFORMATION TECHNOLOGY.—The term
18 “information technology”—

19 (A) has the meaning given the term in sec-
20 tion 11101 of title 40, United States Code; and

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

1 (5) RISK-BASED BUDGET.—The term “risk-
2 based budget” means a budget—

3 (A) developed by identifying and
4 prioritizing cybersecurity risks and
5 vulnerabilities, including impact on agency oper-
6 ations in the case of a cyber attack, through
7 analysis of threat intelligence, incident data,
8 and tactics, techniques, procedures, and capa-
9 bilities of cyber threats; and

10 (B) that allocates resources based on the
11 risks identified and prioritized under subpara-
12 graph (A).

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

14 (a) IN GENERAL.—

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

1 (2) RESPONSIBILITY OF DIRECTOR.—Section
2 3553(a) of title 44, United States Code, is amend-
3 ed—

4 (A) in paragraph (5), by striking “and” at
5 the end;

6 (B) in paragraph (6), by striking the pe-
7 riod at the end and inserting “; and”; and

8 (C) by adding at the end the following:

9 “(7) developing a standard risk-based budget
10 model to inform Federal agency cybersecurity budget
11 development.”.

12 (3) CONTENTS OF MODEL.—The model re-
13 quired to be developed under paragraph (1) shall—

14 (A) consider Federal and non-Federal
15 cyber threat intelligence products, where avail-
16 able, to identify threats, vulnerabilities, and
17 risks;

18 (B) consider the impact of agency oper-
19 ations of compromise of systems, including the
20 interconnectivity to other agency systems and
21 the operations of other agencies;

22 (C) indicate where resources should be al-
23 located to have the greatest impact on miti-
24 gating current and future threats and current
25 and future cybersecurity capabilities;

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

3 (i) information technology and cyber-
4 security tools;

5 (ii) information technology and cyber-
6 security architectures;

7 (iii) information technology and cyber-
8 security personnel; and

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

11 (E) be used to evaluate and inform govern-
12 ment-wide cybersecurity programs of the De-
13 partment of Homeland Security.

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

18 (5) PUBLICATION.—The Director shall publish
19 the model required to be developed under this sub-
20 section, and any updates necessary under paragraph
21 (4), on the public website of the Office of Manage-
22 ment and Budget.

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

1 the date on which the model required to be devel-
 2 oped under this subsection is completed, whichever is
 3 sooner, the Director shall submit a report to Con-
 4 gress on the development of the model.

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

7 (1) IN GENERAL.—Not later than 2 years after
 8 the date on which the model developed under sub-
 9 section (a) is published, the head of each covered
 10 agency shall use the model to develop the annual cy-
 11 bersecurity and information technology budget re-
 12 quests of the agency.

13 (2) AGENCY PERFORMANCE PLANS.—Section
 14 3554(d)(2) of title 44, United States Code, is
 15 amended by inserting “and the risk-based budget
 16 model required under section 3553(a)(7)” after
 17 “paragraph (1)”.

18 (c) VERIFICATION.—

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

21 (A) in the matter preceding subclause (I),
 22 by striking “by agency, and by initiative area
 23 (as determined by the administration)” and in-
 24 serting “and by agency”;

1 (B) in subclause (III), by striking “and”
 2 at the end;

3 (C) in subclause (IV), by adding “and” at
 4 the end; and

5 (D) by adding at the end the following:

6 “(V) a validation that the budg-
 7 ets submitted were developed using a
 8 risk-based methodology;”.

9 (2) EFFECTIVE DATE.—The amendments made
 10 by paragraph (1) shall take effect on the date that
 11 is 2 years after the date on which the model devel-
 12 oped under subsection (a) is published.

13 (d) ANNUAL REPORTS.—

14 (1) ANNUAL INDEPENDENT EVALUATION.—Sec-
 15 tion 3555(a)(2) of title 44, United States Code, is
 16 amended—

17 (A) in subparagraph (B), by striking
 18 “and” at the end;

19 (B) in subparagraph (C), by striking the
 20 period at the end and inserting “; and”; and

21 (C) by adding at the end the following:

22 “(D) an assessment of how the agency im-
 23 plemented the risk-based budget model required
 24 under section 3553(a)(7) and an evaluation of

1 whether the model mitigates agency cyber
2 vulnerabilities.”.

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

5 (A) in paragraph (4), by striking “and” at
6 the end;

7 (B) in paragraph (5), by striking the pe-
8 riod at the end and inserting “; and”; and

9 (C) by adding at the end the following:
10 “(6) an assessment of—

11 “(A) Federal agency implementation of the
12 model required under subsection (a)(7);

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

15 “(C) whether the model mitigates the
16 cyber vulnerabilities of the Federal Govern-
17 ment.”.

18 (e) GAO REPORT.—Not later than 3 years after the
19 date on which the first budget of the President is sub-
20 mitted to Congress containing the validation required
21 under section 1105(a)(35)(A)(i)(V) of title 31, United
22 States Code, as amended by subsection (c), the Comp-
23 troller General of the United States shall submit to the
24 appropriate congressional committees a report that in-
25 cludes—

- 1 (1) an evaluation of the success of covered
2 agencies in developing risk-based budgets;
- 3 (2) an evaluation of the success of covered
4 agencies in implementing risk-based budgets;
- 5 (3) an evaluation of whether the risk-based
6 budgets developed by covered agencies mitigate
7 cyber vulnerability, including the extent to which the
8 risk-based budgets inform Federal Government-wide
9 cybersecurity programs; and
- 10 (4) any other information relating to risk-based
11 budgets the Comptroller General determines appro-
12 priate.

○