



AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: To modernize Federal information security management, to amend the Homeland Security Act of 2002 to require reporting of cyber incidents to the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and to make technical corrections to the Homeland Security Act of 2002.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

### H. R. 4350

To author	AMENDMENT N <sup>o</sup> 4799
activ	
const	By: <i>Peters</i>
ment	To: <i>Amcl. No. 3867</i>
stren	
Referred	
	<i>205</i>
	Page(s)

GPO: 2018 33-682 (mac)

AMENDMENT intended to be proposed by Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, ~~and~~ Ms. COLLINS, *Mr. King and Mr. Rubio*) to the amendment (No. 3867) proposed by Mr. REED

Viz:

1 At the end, add the following:

2 **DIVISION E—FEDERAL INFOR-**

3 **MATION SECURITY MOD-**

4 **ERNIZATION ACT OF 2021**

5 **SEC. 5101. SHORT TITLE.**

6 This division may be cited as the “Federal Informa-

7 tion Security Modernization Act of 2021”.

1 **SEC. 5102. DEFINITIONS.**

2 In this division, unless otherwise specified:

3 (1) **ADDITIONAL CYBERSECURITY PROCE-**  
4 **DURE.**—The term “additional cybersecurity proce-  
5 dure” has the meaning given the term in section  
6 3552(b) of title 44, United States Code, as amended  
7 by this division.

8 (2) **AGENCY.**—The term “agency” has the  
9 meaning given the term in section 3502 of title 44,  
10 United States Code.

11 (3) **APPROPRIATE CONGRESSIONAL COMMIT-**  
12 **TEES.**—The term “appropriate congressional com-  
13 mittees” means—

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

16 (B) the Committee on Oversight and Re-  
17 form of the House of Representatives; and

18 (C) the Committee on Homeland Security  
19 of the House of Representatives.

20 (4) **DIRECTOR.**—The term “Director” means  
21 the Director of the Office of Management and Budg-  
22 et.

23 (5) **INCIDENT.**—The term “incident” has the  
24 meaning given the term in section 3552(b) of title  
25 44, United States Code.

1           (6) NATIONAL SECURITY SYSTEM.—The term  
2           “national security system” has the meaning given  
3           the term in section 3552(b) of title 44, United  
4           States Code.

5           (7) PENETRATION TEST.—The term “penetra-  
6           tion test” has the meaning given the term in section  
7           3552(b) of title 44, United States Code, as amended  
8           by this division.

9           (8) THREAT HUNTING.—The term “threat  
10          hunting” means proactively and iteratively searching  
11          for threats to systems that evade detection by auto-  
12          mated threat detection systems.

## 13       **TITLE LI—UPDATES TO FISMA**

### 14       **SEC. 5121. TITLE 44 AMENDMENTS.**

15          (a) SUBCHAPTER I AMENDMENTS.—Subchapter I of  
16       chapter 35 of title 44, United States Code, is amended—

17               (1) in section 3504—

18                       (A) in subsection (a)(1)(B)—

19                               (i) by striking clause (v) and inserting  
20                               the following:

21                               “(v) confidentiality, privacy, disclosure,  
22                               and sharing of information;”;

23                               (ii) by redesignating clause (vi) as  
24                               clause (vii); and

1 (iii) by inserting after clause (v) the  
2 following:

3 “(vi) in consultation with the National  
4 Cyber Director and the Director of the Cyberse-  
5 curity and Infrastructure Security Agency, se-  
6 curity of information; and”; and

7 (B) in subsection (g), by striking para-  
8 graph (1) and inserting the following:

9 “(1) develop, and in consultation with the Di-  
10 rector of the Cybersecurity and Infrastructure Secu-  
11 rity Agency and the National Cyber Director, over-  
12 see the implementation of policies, principles, stand-  
13 ards, and guidelines on privacy, confidentiality, secu-  
14 rity, disclosure and sharing of information collected  
15 or maintained by or for agencies; and”;

16 (2) in section 3505—

17 (A) in paragraph (3) of the first subsection  
18 designated as subsection (c)—

19 (i) in subparagraph (B)—

20 (I) by inserting “the Director of  
21 the Cybersecurity and Infrastructure  
22 Security Agency, the National Cyber  
23 Director, and” before “the Comp-  
24 troller General”; and

25 (II) by striking “and” at the end;

1 (ii) in subparagraph (C)(v), by strik-  
2 ing the period at the end and inserting “;  
3 and”; and

4 (iii) by adding at the end the fol-  
5 lowing:

6 “(D) maintained on a continual basis through  
7 the use of automation, machine-readable data, and  
8 scanning.”; and

9 (B) by striking the second subsection des-  
10 ignated as subsection (c);

11 (3) in section 3506—

12 (A) in subsection (b)(1)(C), by inserting “,  
13 availability” after “integrity”; and

14 (B) in subsection (h)(3), by inserting “se-  
15 curity,” after “efficiency,”; and

16 (4) in section 3513—

17 (A) by redesignating subsection (c) as sub-  
18 section (d); and

19 (B) by inserting after subsection (b) the  
20 following:

21 “(c) Each agency providing a written plan under sub-  
22 section (b) shall provide any portion of the written plan  
23 addressing information security or cybersecurity to the Di-  
24 rector of the Cybersecurity and Infrastructure Security  
25 Agency.”.

1 (b) SUBCHAPTER II DEFINITIONS.—

2 (1) IN GENERAL.—Section 3552(b) of title 44,  
3 United States Code, is amended—

4 (A) by redesignating paragraphs (1), (2),  
5 (3), (4), (5), (6), and (7) as paragraphs (2),  
6 (3), (4), (5), (6), (9), and (11), respectively;

7 (B) by inserting before paragraph (2), as  
8 so redesignated, the following:

9 “(1) The term ‘additional cybersecurity proce-  
10 dure’ means a process, procedure, or other activity  
11 that is established in excess of the information secu-  
12 rity standards promulgated under section 11331(b)  
13 of title 40 to increase the security and reduce the cy-  
14 bersecurity risk of agency systems.”;

15 (C) by inserting after paragraph (6), as so  
16 redesignated, the following:

17 “(7) The term ‘high value asset’ means infor-  
18 mation or an information system that the head of an  
19 agency determines so critical to the agency that the  
20 loss or corruption of the information or the loss of  
21 access to the information system would have a seri-  
22 ous impact on the ability of the agency to perform  
23 the mission of the agency or conduct business.

1           “(8) The term ‘major incident’ has the meaning  
2           given the term in guidance issued by the Director  
3           under section 3598(a).”;

4           (D) by inserting after paragraph (9), as so  
5           redesignated, the following:

6           “(10) The term ‘penetration test’ means a spe-  
7           cialized type of assessment that—

8           “(A) is conducted on an information sys-  
9           tem or a component of an information system;  
10          and

11          “(B) emulates an attack or other exploi-  
12          tation capability of a potential adversary, typi-  
13          cally under specific constraints, in order to  
14          identify any vulnerabilities of an information  
15          system or a component of an information sys-  
16          tem that could be exploited.”; and

17          (E) by inserting after paragraph (11), as  
18          so redesignated, the following:

19          “(12) The term ‘shared service’ means a cen-  
20          tralized business or mission capability that is pro-  
21          vided to multiple organizations within an agency or  
22          to multiple agencies.”.

23          (2) CONFORMING AMENDMENTS.—

24                 (A) HOMELAND SECURITY ACT OF 2002.—  
25          Section 1001(c)(1)(A) of the Homeland Secu-

1           rity Act of 2002 (6 U.S.C. 511(1)(A)) is  
2           amended by striking “section 3552(b)(5)” and  
3           inserting “section 3552(b)”.

4           (B) TITLE 10.—

5                 (i) SECTION 2222.—Section 2222(i)(8)  
6                 of title 10, United States Code, is amended  
7                 by striking “section 3552(b)(6)(A)” and  
8                 inserting “section 3552(b)(9)(A)”.

9                 (ii)         SECTION         2223.—Section  
10                2223(c)(3) of title 10, United States Code,  
11                is amended by striking “section  
12                3552(b)(6)” and inserting “section  
13                3552(b)”.

14               (iii) SECTION 2315.—Section 2315 of  
15                title 10, United States Code, is amended  
16                by striking “section 3552(b)(6)” and in-  
17                serting “section 3552(b)”.

18               (iv)         SECTION         2339A.—Section  
19                2339a(e)(5) of title 10, United States  
20                Code, is amended by striking “section  
21                3552(b)(6)” and inserting “section  
22                3552(b)”.

23           (C) HIGH-PERFORMANCE COMPUTING ACT  
24           OF 1991.—Section 207(a) of the High-Perform-  
25           ance Computing Act of 1991 (15 U.S.C.



1           5527(a)) is amended by striking “section  
2           3552(b)(6)(A)(i)” and inserting “section  
3           3552(b)(9)(A)(i)”.

4           (D) INTERNET OF THINGS CYBERSECURITY  
5           IMPROVEMENT ACT OF 2020.—Section 3(5)  
6           of the Internet of Things Cybersecurity Im-  
7           provement Act of 2020 (15 U.S.C. 278g–3a) is  
8           amended by striking “section 3552(b)(6)” and  
9           inserting “section 3552(b)”.

10          (E) NATIONAL DEFENSE AUTHORIZATION  
11          ACT FOR FISCAL YEAR 2013.—Section  
12          933(e)(1)(B) of the National Defense Author-  
13          ization Act for Fiscal Year 2013 (10 U.S.C.  
14          2224 note) is amended by striking “section  
15          3542(b)(2)” and inserting “section 3552(b)”.

16          (F) IKE SKELTON NATIONAL DEFENSE AU-  
17          THORIZATION ACT FOR FISCAL YEAR 2011.—The  
18          Ike Skelton National Defense Authorization Act  
19          for Fiscal Year 2011 (Public Law 111–383) is  
20          amended—

21               (i) in section 806(e)(5) (10 U.S.C.  
22               2304 note), by striking “section 3542(b)”  
23               and inserting “section 3552(b)”;

24               (ii) in section 931(b)(3) (10 U.S.C.  
25               2223 note), by striking “section

1                   3542(b)(2)” and inserting “section  
2                   3552(b)”;

3                   (iii) in section 932(b)(2) (10 U.S.C.  
4                   2224 note), by striking “section  
5                   3542(b)(2)” and inserting “section  
6                   3552(b)”.

7                   (G) E-GOVERNMENT ACT OF 2002.—Sec-  
8                   tion 301(c)(1)(A) of the E-Government Act of  
9                   2002 (44 U.S.C. 3501 note) is amended by  
10                  striking “section 3542(b)(2)” and inserting  
11                  “section 3552(b)”.

12                  (H) NATIONAL INSTITUTE OF STANDARDS  
13                  AND TECHNOLOGY ACT.—Section 20 of the Na-  
14                  tional Institute of Standards and Technology  
15                  Act (15 U.S.C. 278g-3) is amended—

16                  (i) in subsection (a)(2), by striking  
17                  “section 3552(b)(5)” and inserting “sec-  
18                  tion 3552(b)”;

19                  (ii) in subsection (f)—

20                  (I) in paragraph (3), by striking  
21                  “section 3532(1)” and inserting “sec-  
22                  tion 3552(b)”;

23                  (II) in paragraph (5), by striking  
24                  “section 3532(b)(2)” and inserting  
25                  “section 3552(b)”.

1 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II  
2 of chapter 35 of title 44, United States Code, is amend-  
3 ed—

4 (1) in section 3551—

5 (A) in paragraph (4), by striking “diag-  
6 nose and improve” and inserting “integrate, de-  
7 liver, diagnose, and improve”;

8 (B) in paragraph (5), by striking “and” at  
9 the end;

10 (C) in paragraph (6), by striking the pe-  
11 riod at the end and inserting a semi colon; and

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

13 “(7) recognize that each agency has specific  
14 mission requirements and, at times, unique cyberse-  
15 curity requirements to meet the mission of the agen-  
16 cy;

17 “(8) recognize that each agency does not have  
18 the same resources to secure agency systems, and an  
19 agency should not be expected to have the capability  
20 to secure the systems of the agency from advanced  
21 adversaries alone; and

22 “(9) recognize that a holistic Federal cybersecu-  
23 rity model is necessary to account for differences be-  
24 tween the missions and capabilities of agencies.”;

25 (2) in section 3553—

1 (A) by striking the section heading and in-  
2 serting “**Authority and functions of the**  
3 **Director and the Director of the Cy-**  
4 **bersecurity and Infrastructure Secu-**  
5 **rity Agency**”.

6 (B) in subsection (a)—

7 (i) in paragraph (1), by inserting “, in  
8 consultation with the Director of the Cy-  
9 bersecurity and Infrastructure Security  
10 Agency and the National Cyber Director,”  
11 before “overseeing”;

12 (ii) in paragraph (5), by striking  
13 “and” at the end; and

14 (iii) by adding at the end the fol-  
15 lowing:

16 “(8) promoting, in consultation with the Direc-  
17 tor of the Cybersecurity and Infrastructure Security  
18 Agency and the Director of the National Institute of  
19 Standards and Technology—

20 “(A) the use of automation to improve  
21 Federal cybersecurity and visibility with respect  
22 to the implementation of Federal cybersecurity;  
23 and

24 “(B) the use of presumption of com-  
25 promise and least privilege principles to improve

- 1           resiliency and timely response actions to inci-  
2           dents on Federal systems.”;
- 3           (C) in subsection (b)—
- 4           (i) by striking the subsection heading  
5           and inserting “CYBERSECURITY AND IN-  
6           FRASTRUCTURE SECURITY AGENCY”;
- 7           (ii) in the matter preceding paragraph  
8           (1), by striking “The Secretary, in con-  
9           sultation with the Director” and inserting  
10          “The Director of the Cybersecurity and In-  
11          frastructure Security Agency, in consulta-  
12          tion with the Director and the National  
13          Cyber Director”;
- 14          (iii) in paragraph (2)—
- 15          (I) in subparagraph (A), by in-  
16          serting “and reporting requirements  
17          under subchapter IV of this title”  
18          after “section 3556”; and
- 19          (II) in subparagraph (D), by  
20          striking “the Director or Secretary”  
21          and inserting “the Director of the Cy-  
22          bersecurity and Infrastructure Secu-  
23          rity Agency”;

1 (iv) in paragraph (5), by striking “co-  
2 ordinating” and inserting “leading the co-  
3 ordination of”;

4 (v) in paragraph (8), by striking “the  
5 Secretary’s discretion” and inserting “the  
6 Director of the Cybersecurity and Infra-  
7 structure Security Agency’s discretion”;  
8 and

9 (vi) in paragraph (9), by striking “as  
10 the Director or the Secretary, in consulta-  
11 tion with the Director,” and inserting “as  
12 the Director of the Cybersecurity and In-  
13 frastructure Security Agency”;

14 (D) in subsection (c)—

15 (i) in the matter preceding paragraph  
16 (1), by striking “each year” and inserting  
17 “each year during which agencies are re-  
18 quired to submit reports under section  
19 3554(c)”;

20 (ii) by striking paragraph (1);

21 (iii) by redesignating paragraphs (2),  
22 (3), and (4) as paragraphs (1), (2), and  
23 (3), respectively;

24 (iv) in paragraph (3), as so redesign-  
25 nated, by striking “and” at the end;

1 (v) by inserting after paragraph (3),  
2 as so redesignated the following:

3 “(4) a summary of each assessment of Federal  
4 risk posture performed under subsection (i);” and

5 (vi) in paragraph (5), by striking the  
6 period at the end and inserting “; and”;

7 (E) by redesignating subsections (i), (j),  
8 (k), and (l) as subsections (j), (k), (l), and (m)  
9 respectively;

10 (F) by inserting after subsection (h) the  
11 following:

12 “(i) FEDERAL RISK ASSESSMENTS.—On an ongoing  
13 and continuous basis, the Director of the Cybersecurity  
14 and Infrastructure Security Agency shall perform assess-  
15 ments of Federal risk posture using any available informa-  
16 tion on the cybersecurity posture of agencies, and brief  
17 the Director and National Cyber Director on the findings  
18 of those assessments including—

19 “(1) the status of agency cybersecurity remedial  
20 actions described in section 3554(b)(7);

21 “(2) any vulnerability information relating to  
22 the systems of an agency that is known by the agen-  
23 cy;

24 “(3) analysis of incident information under sec-  
25 tion 3597;

1           “(4) evaluation of penetration testing per-  
2           formed under section 3559A;

3           “(5) evaluation of vulnerability disclosure pro-  
4           gram information under section 3559B;

5           “(6) evaluation of agency threat hunting re-  
6           sults;

7           “(7) evaluation of Federal and non-Federal  
8           cyber threat intelligence;

9           “(8) data on agency compliance with standards  
10          issued under section 11331 of title 40;

11          “(9) agency system risk assessments performed  
12          under section 3554(a)(1)(A); and

13          “(10) any other information the Director of the  
14          Cybersecurity and Infrastructure Security Agency  
15          determines relevant.”; and

16               (G) in subsection (j), as so redesignated—

17                   (i) by striking “regarding the spe-  
18                   cific” and inserting “that includes a sum-  
19                   mary of—

20                   “(1) the specific”;

21                   (ii) in paragraph (1), as so des-  
22                   ignated, by striking the period at the end  
23                   and inserting “; and” and

24                   (iii) by adding at the end the fol-  
25                   lowing:



1           “(2) the trends identified in the Federal risk  
2           assessment performed under subsection (i).”; and

3                       (H) by adding at the end the following:

4           “(n) BINDING OPERATIONAL DIRECTIVES.—If the  
5           Director of the Cybersecurity and Infrastructure Security  
6           Agency issues a binding operational directive or an emer-  
7           gency directive under this section, not later than 2 days  
8           after the date on which the binding operational directive  
9           requires an agency to take an action, the Director of the  
10          Cybersecurity and Infrastructure Security Agency shall  
11          provide to the appropriate reporting entities the status of  
12          the implementation of the binding operational directive at  
13          the agency.”;

14                       (3) in section 3554—

15                               (A) in subsection (a)—

16                                       (i) in paragraph (1)—

17   (I) by redesignating subpara-  
18   graphs (A), (B), and (C) as subpara-  
19   graphs (B), (C), and (D), respectively;

20   (II) by inserting before subpara-  
21   graph (B), as so redesignated, the fol-  
22   lowing:

23                               “(A) on an ongoing and continuous basis,  
24                       performing agency system risk assessments  
25                       that—

1 “(i) identify and document the high  
2 value assets of the agency using guidance  
3 from the Director;

4 “(ii) evaluate the data assets inven-  
5 toried under section 3511 for sensitivity to  
6 compromises in confidentiality, integrity,  
7 and availability;

8 “(iii) identify agency systems that  
9 have access to or hold the data assets  
10 inventoried under section 3511;

11 “(iv) evaluate the threats facing agen-  
12 cy systems and data, including high value  
13 assets, based on Federal and non-Federal  
14 cyber threat intelligence products, where  
15 available;

16 “(v) evaluate the vulnerability of  
17 agency systems and data, including high  
18 value assets, including by analyzing—

19 “(I) the results of penetration  
20 testing performed by the Department  
21 of Homeland Security under section  
22 3553(b)(9);

23 “(II) the results of penetration  
24 testing performed under section  
25 3559A;

1                   “(III) information provided to  
2                   the agency through the vulnerability  
3                   disclosure program of the agency  
4                   under section 3559B;  
5                   “(IV) incidents; and  
6                   “(V) any other vulnerability in-  
7                   formation relating to agency systems  
8                   that is known to the agency;  
9                   “(vi) assess the impacts of potential  
10                  agency incidents to agency systems, data,  
11                  and operations based on the evaluations  
12                  described in clauses (ii) and (iv) and the  
13                  agency systems identified under clause  
14                  (iii); and  
15                  “(vii) assess the consequences of po-  
16                  tential incidents occurring on agency sys-  
17                  tems that would impact systems at other  
18                  agencies, including due to interconnectivity  
19                  between different agency systems or oper-  
20                  ational reliance on the operations of the  
21                  system or data in the system;”;  
22                  (III) in subparagraph (B), as so  
23                  redesignated, in the matter preceding  
24                  clause (i), by striking “providing in-  
25                  formation” and inserting “using infor-

1                   mation from the assessment con-  
2                   ducted under subparagraph (A), pro-  
3                   viding, in consultation with the Direc-  
4                   tor of the Cybersecurity and Infra-  
5                   structure Security Agency, informa-  
6                   tion”;

7                   (IV) in subparagraph (C), as so  
8                   redesignated—

9                   (aa) in clause (ii) by insert-  
10                  ing “binding” before “oper-  
11                  ational”; and

12                  (bb) in clause (vi), by strik-  
13                  ing “and” at the end; and

14                  (V) by adding at the end the fol-  
15                  lowing:

16                  “(E) providing an update on the ongoing  
17                  and continuous assessment performed under  
18                  subparagraph (A)—

19                  “(i) upon request, to the inspector  
20                  general of the agency or the Comptroller  
21                  General of the United States; and

22                  “(ii) on a periodic basis, as deter-  
23                  mined by guidance issued by the Director  
24                  but not less frequently than annually, to—

25                  “(I) the Director;

## 21

1                   “(II) the Director of the Cyberse-  
2                   curity and Infrastructure Security  
3                   Agency; and

4                   “(III) the National Cyber Direc-  
5                   tor;

6                   “(F) in consultation with the Director of  
7                   the Cybersecurity and Infrastructure Security  
8                   Agency and not less frequently than once every  
9                   3 years, performing an evaluation of whether  
10                  additional cybersecurity procedures are appro-  
11                  priate for securing a system of, or under the  
12                  supervision of, the agency, which shall—

13                  “(i) be completed considering the  
14                  agency system risk assessment performed  
15                  under subparagraph (A); and

16                  “(ii) include a specific evaluation for  
17                  high value assets;

18                  “(G) not later than 30 days after com-  
19                  pleting the evaluation performed under sub-  
20                  paragraph (F), providing the evaluation and an  
21                  implementation plan, if applicable, for using ad-  
22                  ditional cybersecurity procedures determined to  
23                  be appropriate to—

24                  “(i) the Director of the Cybersecurity  
25                  and Infrastructure Security Agency;

1 “(ii) the Director; and

2 “(iii) the National Cyber Director;

3 and

4 “(H) if the head of the agency determines  
5 there is need for additional cybersecurity proce-  
6 dures, ensuring that those additional cybersecu-  
7 rity procedures are reflected in the budget re-  
8 quest of the agency in accordance with the risk-  
9 based cyber budget model developed pursuant  
10 to section 3553(a)(7);”;

11 (ii) in paragraph (2)—

12 (I) in subparagraph (A), by in-  
13 serting “in accordance with the agen-  
14 cy system risk assessment performed  
15 under paragraph (1)(A)” after “infor-  
16 mation systems”;

17 (II) in subparagraph (B)—

18 (aa) by striking “in accord-  
19 ance with standards” and insert-  
20 ing “in accordance with—

21 “(i) standards”; and

22 (bb) by adding at the end  
23 the following:

24 “(ii) the evaluation performed under  
25 paragraph (1)(F); and

1                   “(iii) the implementation plan de-  
2                   scribed in paragraph (1)(G);”; and

3                   (III) in subparagraph (D), by in-  
4                   serting “, through the use of penetra-  
5                   tion testing, the vulnerability disclo-  
6                   sure program established under sec-  
7                   tion 3559B, and other means,” after  
8                   “periodically”;

9                   (iii) in paragraph (3)—

10                  (I) in subparagraph (A)—

11                   (aa) in clause (iii), by strik-  
12                   ing “and” at the end;

13                   (bb) in clause (iv), by add-  
14                   ing “and” at the end; and

15                   (cc) by adding at the end  
16                   the following:

17                  “(v) ensure that—

18                   “(I) senior agency information  
19                   security officers of component agen-  
20                   cies carry out responsibilities under  
21                   this subchapter, as directed by the  
22                   senior agency information security of-  
23                   ficer of the agency or an equivalent  
24                   official; and

1 “(II) senior agency information  
2 security officers of component agen-  
3 cies report to—

4 “(aa) the senior information  
5 security officer of the agency or  
6 an equivalent official; and

7 “(bb) the Chief Information  
8 Officer of the component agency  
9 or an equivalent official;”; and

10 (iv) in paragraph (5), by inserting  
11 “and the Director of the Cybersecurity and  
12 Infrastructure Security Agency” before  
13 “on the effectiveness”;

14 (B) in subsection (b)—

15 (i) by striking paragraph (1) and in-  
16 serting the following:

17 “(1) pursuant to subsection (a)(1)(A), per-  
18 forming ongoing and continuous agency system risk  
19 assessments, which may include using guidelines and  
20 automated tools consistent with standards and  
21 guidelines promulgated under section 11331 of title  
22 40, as applicable;”;

23 (ii) in paragraph (2)—

24 (I) by striking subparagraph (B)  
25 and inserting the following:



1 “(B) comply with the risk-based cyber  
2 budget model developed pursuant to section  
3 3553(a)(7);” and

4 (II) in subparagraph (D)—

5 (aa) by redesignating  
6 clauses (iii) and (iv) as clauses  
7 (iv) and (v), respectively;

8 (bb) by inserting after  
9 clause (ii) the following:

10 “(iii) binding operational directives  
11 and emergency directives promulgated by  
12 the Director of the Cybersecurity and In-  
13 frastructure Security Agency under section  
14 3553;” and

15 (cc) in clause (iv), as so re-  
16 designated, by striking “as deter-  
17 mined by the agency; and” and  
18 inserting “as determined by the  
19 agency, considering—

20 “(I) the agency risk assessment  
21 performed under subsection (a)(1)(A);  
22 and

23 “(II) the determinations of ap-  
24 plying more stringent standards and  
25 additional cybersecurity procedures

1                   pursuant to section 11331(c)(1) of  
2                   title 40; and”;

3                   (iii) in paragraph (5)(A), by inserting  
4                   “, including penetration testing, as appro-  
5                   priate,” after “shall include testing”;

6                   (iv) in paragraph (6), by striking  
7                   “planning, implementing, evaluating, and  
8                   documenting” and inserting “planning and  
9                   implementing and, in consultation with the  
10                  Director of the Cybersecurity and Infra-  
11                  structure Security Agency, evaluating and  
12                  documenting”;

13                  (v) by redesignating paragraphs (7)  
14                  and (8) as paragraphs (8) and (9), respec-  
15                  tively;

16                  (vi) by inserting after paragraph (6)  
17                  the following:

18                  “(7) a process for providing the status of every  
19                  remedial action and known system vulnerability to  
20                  the Director and the Director of the Cybersecurity  
21                  and Infrastructure Security Agency, using automa-  
22                  tion and machine-readable data to the greatest ex-  
23                  tent practicable;” and

24                  (vii) in paragraph (8)(C), as so redes-  
25                  ignated—

## 27

1 (I) by striking clause (ii) and in-  
2 serting the following:

3 “(ii) notifying and consulting with the  
4 Federal information security incident cen-  
5 ter established under section 3556 pursu-  
6 ant to the requirements of section 3594;”;

7 (II) by redesignating clause (iii)  
8 as clause (iv);

9 (III) by inserting after clause (ii)  
10 the following:

11 “(iii) performing the notifications and  
12 other activities required under subchapter  
13 IV of this title; and”; and

14 (IV) in clause (iv), as so redesign-  
15 nated—

16 (aa) in subclause (I), by  
17 striking “and relevant offices of  
18 inspectors general”;

19 (bb) in subclause (II), by  
20 adding “and” at the end;

21 (cc) by striking subclause  
22 (III); and

23 (dd) by redesignating sub-  
24 clause (IV) as subclause (III);

25 (C) in subsection (c)—

1 (i) by redesignating paragraph (2) as  
2 paragraph (5);

3 (ii) by striking paragraph (1) and in-  
4 serting the following:

5 “(1) BIENNIAL REPORT.—Not later than 2  
6 years after the date of enactment of the Federal In-  
7 formation Security Modernization Act of 2021 and  
8 not less frequently than once every 2 years there-  
9 after, using the continuous and ongoing agency sys-  
10 tem risk assessment under subsection (a)(1)(A), the  
11 head of each agency shall submit to the Director,  
12 the Director of the Cybersecurity and Infrastructure  
13 Security Agency, the majority and minority leaders  
14 of the Senate, the Speaker and minority leader of  
15 the House of Representatives, the Committee on  
16 Homeland Security and Governmental Affairs of the  
17 Senate, the Committee on Oversight and Reform of  
18 the House of Representatives, the Committee on  
19 Homeland Security of the House of Representatives,  
20 the Committee on Commerce, Science, and Trans-  
21 portation of the Senate, the Committee on Science,  
22 Space, and Technology of the House of Representa-  
23 tives, the appropriate authorization and appropri-  
24 ations committees of Congress, the National Cyber

1 Director, and the Comptroller General of the United  
2 States a report that—

3 “(A) summarizes the agency system risk  
4 assessment performed under subsection  
5 (a)(1)(A);

6 “(B) evaluates the adequacy and effective-  
7 ness of information security policies, proce-  
8 dures, and practices of the agency to address  
9 the risks identified in the agency system risk  
10 assessment performed under subsection  
11 (a)(1)(A), including an analysis of the agency’s  
12 cybersecurity and incident response capabilities  
13 using the metrics established under section  
14 224(e) of the Cybersecurity Act of 2015 (6  
15 U.S.C. 1522(e));

16 “(C) summarizes the evaluation and imple-  
17 mentation plans described in subparagraphs (F)  
18 and (G) of subsection (a)(1) and whether those  
19 evaluation and implementation plans call for  
20 the use of additional cybersecurity procedures  
21 determined to be appropriate by the agency;  
22 and

23 “(D) summarizes the status of remedial  
24 actions identified by inspector general of the  
25 agency, the Comptroller General of the United

1 States, and any other source determined appro-  
2 priate by the head of the agency.

3 “(2) UNCLASSIFIED REPORTS.—Each report  
4 submitted under paragraph (1)—

5 “(A) shall be, to the greatest extent prac-  
6 ticable, in an unclassified and otherwise uncon-  
7 trolled form; and

8 “(B) may include a classified annex.

9 “(3) ACCESS TO INFORMATION.—The head of  
10 an agency shall ensure that, to the greatest extent  
11 practicable, information is included in the unclassi-  
12 fied form of the report submitted by the agency  
13 under paragraph (2)(A).

14 “(4) BRIEFINGS.—During each year during  
15 which a report is not required to be submitted under  
16 paragraph (1), the Director shall provide to the con-  
17 gressional committees described in paragraph (1) a  
18 briefing summarizing current agency and Federal  
19 risk postures.”; and

20 (iii) in paragraph (5), as so redesign-  
21 nated, by striking the period at the end  
22 and inserting “, including the reporting  
23 procedures established under section  
24 11315(d) of title 40 and subsection  
25 (a)(3)(A)(v) of this section.”; and

1 (D) in subsection (d)(1), in the matter pre-  
2 ceding subparagraph (A), by inserting “and the  
3 Director of the Cybersecurity and Infrastruc-  
4 ture Security Agency” after “the Director”; and  
5 (4) in section 3555—

6 (A) in the section heading, by striking  
7 “**ANNUAL INDEPENDENT**” and inserting  
8 “**INDEPENDENT**”;

9 (B) in subsection (a)—

10 (i) in paragraph (1), by inserting  
11 “during which a report is required to be  
12 submitted under section 3553(c),” after  
13 “Each year”;

14 (ii) in paragraph (2)(A), by inserting  
15 “, including by penetration testing and  
16 analyzing the vulnerability disclosure pro-  
17 gram of the agency” after “information  
18 systems”; and

19 (iii) by adding at the end the fol-  
20 lowing:

21 “(3) An evaluation under this section may include  
22 recommendations for improving the cybersecurity posture  
23 of the agency.”;

24 (C) in subsection (b)(1), by striking “an-  
25 nual”;

1 (D) in subsection (e)(1), by inserting “dur-  
2 ing which a report is required to be submitted  
3 under section 3553(c)” after “Each year”;

4 (E) by striking subsection (f) and inserting  
5 the following:

6 “(f) PROTECTION OF INFORMATION.—(1) Agencies,  
7 evaluators, and other recipients of information that, if dis-  
8 closed, may cause grave harm to the efforts of Federal  
9 information security officers shall take appropriate steps  
10 to ensure the protection of that information, including  
11 safeguarding the information from public disclosure.

12 “(2) The protections required under paragraph (1)  
13 shall be commensurate with the risk and comply with all  
14 applicable laws and regulations.

15 “(3) With respect to information that is not related  
16 to national security systems, agencies and evaluators shall  
17 make a summary of the information unclassified and pub-  
18 licly available, including information that does not iden-  
19 tify—

20 “(A) specific information system incidents; or

21 “(B) specific information system  
22 vulnerabilities.”;

23 (F) in subsection (g)(2)—

24 (i) by striking “this subsection shall”  
25 and inserting “this subsection—



1 “(A) shall”;

2 (ii) in subparagraph (A), as so des-  
3 ignated, by striking the period at the end  
4 and inserting “; and”; and

5 (iii) by adding at the end the fol-  
6 lowing:

7 “(B) identify any entity that performs an inde-  
8 pendent evaluation under subsection (b).”; and

9 (G) by striking subsection (j) and inserting  
10 the following:

11 “(j) GUIDANCE.—

12 “(1) IN GENERAL.—The Director, in consulta-  
13 tion with the Director of the Cybersecurity and In-  
14 frastructure Security Agency, the Chief Information  
15 Officers Council, the Council of the Inspectors Gen-  
16 eral on Integrity and Efficiency, and other interested  
17 parties as appropriate, shall ensure the development  
18 of guidance for evaluating the effectiveness of an in-  
19 formation security program and practices

20 “(2) PRIORITIES.—The guidance developed  
21 under paragraph (1) shall prioritize the identifica-  
22 tion of—

23 “(A) the most common threat patterns ex-  
24 perience by each agency;

1 “(B) the security controls that address the  
2 threat patterns described in subparagraph (A);  
3 and

4 “(C) any other security risks unique to the  
5 networks of each agency.”; and  
6 (5) in section 3556(a)—

7 (A) in the matter preceding paragraph (1),  
8 by inserting “within the Cybersecurity and In-  
9 frastructure Security Agency” after “incident  
10 center”; and

11 (B) in paragraph (4), by striking  
12 “3554(b)” and inserting “3554(a)(1)(A)”.

13 (d) CONFORMING AMENDMENTS.—

14 (1) TABLE OF SECTIONS.—The table of sections  
15 for chapter 35 of title 44, United States Code, is  
16 amended—

17 (A) by striking the item relating to section  
18 3553 and inserting the following:

“3553. Authority and functions of the Director and the Director of the Cyberse-  
curity and Infrastructure Security Agency.”; and

19 (B) by striking the item relating to section  
20 3555 and inserting the following:

“3555. Independent evaluation.”.

21 (2) OMB REPORTS.—Section 226(c) of the Cy-  
22 bersecurity Act of 2015 (6 U.S.C. 1524(c)) is  
23 amended—

## 35

1 (A) in paragraph (1)(B), in the matter  
2 preceding clause (i), by striking “annually  
3 thereafter” and inserting “thereafter during the  
4 years during which a report is required to be  
5 submitted under section 3553(c) of title 44,  
6 United States Code”; and

7 (B) in paragraph (2)(B), in the matter  
8 preceding clause (i)—

9 (i) by striking “annually thereafter”  
10 and inserting “thereafter during the years  
11 during which a report is required to be  
12 submitted under section 3553(c) of title  
13 44, United States Code”; and

14 (ii) by striking “the report required  
15 under section 3553(c) of title 44, United  
16 States Code” and inserting “that report”.

17 (3) NIST RESPONSIBILITIES.—Section  
18 20(d)(3)(B) of the National Institute of Standards  
19 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is  
20 amended by striking “annual”.

21 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

22 (1) IN GENERAL.—Chapter 35 of title 44,  
23 United States Code, is amended by adding at the  
24 end the following:

1           “SUBCHAPTER IV—FEDERAL SYSTEM  
2                           INCIDENT RESPONSE

3   **“§ 3591. Definitions**

4           “(a) IN GENERAL.—Except as provided in subsection  
5 (b), the definitions under sections 3502 and 3552 shall  
6 apply to this subchapter.

7           “(b) ADDITIONAL DEFINITIONS.—As used in this  
8 subchapter:

9                   “(1) APPROPRIATE REPORTING ENTITIES.—The  
10 term ‘appropriate reporting entities’ means—

11                           “(A) the majority and minority leaders of  
12 the Senate;

13                           “(B) the Speaker and minority leader of  
14 the House of Representatives;

15                           “(C) the Committee on Homeland Security  
16 and Governmental Affairs of the Senate;

17                           “(D) the Committee on Oversight and Re-  
18 form of the House of Representatives;

19                           “(E) the Committee on Homeland Security  
20 of the House of Representatives;

21                           “(F) the appropriate authorization and ap-  
22 propriations committees of Congress;

23                           “(G) the Director;

24                           “(H) the Director of the Cybersecurity and  
25 Infrastructure Security Agency;

1 “(I) the National Cyber Director;

2 “(J) the Comptroller General of the United  
3 States; and

4 “(K) the inspector general of any impacted  
5 agency.

6 “(2) AWARDEE.—The term ‘awardee’—

7 “(A) means a person, business, or other  
8 entity that receives a grant from, or is a party  
9 to a cooperative agreement or an other trans-  
10 action agreement with, an agency; and

11 “(B) includes any subgrantee of a person,  
12 business, or other entity described in subpara-  
13 graph (A).

14 “(3) BREACH.—The term ‘breach’ means—

15 “(A) a compromise of the security, con-  
16 fidentiality, or integrity of data in electronic  
17 form that results in unauthorized access to, or  
18 an acquisition of, personal information; or

19 “(B) a loss of data in electronic form that  
20 results in unauthorized access to, or an acqui-  
21 sition of, personal information.

22 “(4) CONTRACTOR.—The term ‘contractor’  
23 means—

1           “(A) a prime contractor of an agency or a  
2           subcontractor of a prime contractor of an agen-  
3           cy; and

4           “(B) any person or business that collects  
5           or maintains information, including personally  
6           identifiable information, on behalf of an agency.

7           “(5) FEDERAL INFORMATION.—The term ‘Fed-  
8           eral information’ means information created, col-  
9           lected, processed, maintained, disseminated, dis-  
10          closed, or disposed of by or for the Federal Govern-  
11          ment in any medium or form.

12          “(6) FEDERAL INFORMATION SYSTEM.—The  
13          term ‘Federal information system’ means an infor-  
14          mation system used or operated by an agency, a con-  
15          tractor, an awardee, or another organization on be-  
16          half of an agency.

17          “(7) INTELLIGENCE COMMUNITY.—The term  
18          ‘intelligence community’ has the meaning given the  
19          term in section 3 of the National Security Act of  
20          1947 (50 U.S.C. 3003).

21          “(8) NATIONWIDE CONSUMER REPORTING  
22          AGENCY.—The term ‘nationwide consumer reporting  
23          agency’ means a consumer reporting agency de-  
24          scribed in section 603(p) of the Fair Credit Report-  
25          ing Act (15 U.S.C. 1681a(p)).

1           “(9) VULNERABILITY DISCLOSURE.—The term  
2           ‘vulnerability disclosure’ means a vulnerability iden-  
3           tified under section 3559B.

4   **“§ 3592. Notification of breach**

5           “(a) NOTIFICATION.—As expeditiously as practicable  
6           and without unreasonable delay, and in any case not later  
7           than 45 days after an agency has a reasonable basis to  
8           conclude that a breach has occurred, the head of the agen-  
9           cy, in consultation with a senior privacy officer of the  
10          agency, shall—

11           “(1) determine whether notice to any individual  
12          potentially affected by the breach is appropriate  
13          based on an assessment of the risk of harm to the  
14          individual that considers—

15           “(A) the nature and sensitivity of the per-  
16          sonally identifiable information affected by the  
17          breach;

18           “(B) the likelihood of access to and use of  
19          the personally identifiable information affected  
20          by the breach;

21           “(C) the type of breach; and

22           “(D) any other factors determined by the  
23          Director; and

1           “(2) as appropriate, provide written notice in  
2           accordance with subsection (b) to each individual po-  
3           tentially affected by the breach—

4                   “(A) to the last known mailing address of  
5           the individual; or

6                   “(B) through an appropriate alternative  
7           method of notification that the head of the  
8           agency or a designated senior-level individual of  
9           the agency selects based on factors determined  
10          by the Director.

11          “(b) CONTENTS OF NOTICE.—Each notice of a  
12          breach provided to an individual under subsection (a)(2)  
13          shall include—

14                  “(1) a brief description of the rationale for the  
15          determination that notice should be provided under  
16          subsection (a);

17                  “(2) if possible, a description of the types of  
18          personally identifiable information affected by the  
19          breach;

20                  “(3) contact information of the agency that  
21          may be used to ask questions of the agency, which—

22                          “(A) shall include an e-mail address or an-  
23                  other digital contact mechanism; and

24                          “(B) may include a telephone number or a  
25                  website;



1           “(4) information on any remedy being offered  
2       by the agency;

3           “(5) any applicable educational materials relat-  
4       ing to what individuals can do in response to a  
5       breach that potentially affects their personally iden-  
6       tifiable information, including relevant contact infor-  
7       mation for Federal law enforcement agencies and  
8       each nationwide consumer reporting agency; and

9           “(6) any other appropriate information, as de-  
10       termined by the head of the agency or established in  
11       guidance by the Director.

12       “(c) DELAY OF NOTIFICATION.—

13           “(1) IN GENERAL.—The Attorney General, the  
14       Director of National Intelligence, or the Secretary of  
15       Homeland Security may delay a notification required  
16       under subsection (a) if the notification would—

17           “(A) impede a criminal investigation or a  
18       national security activity;

19           “(B) reveal sensitive sources and methods;

20           “(C) cause damage to national security; or

21           “(D) hamper security remediation actions.

22       “(2) DOCUMENTATION.—

23           “(A) IN GENERAL.—Any delay under para-  
24       graph (1) shall be reported in writing to the Di-  
25       rector, the Attorney General, the Director of

1 National Intelligence, the Secretary of Home-  
2 land Security, the Director of the Cybersecurity  
3 and Infrastructure Security Agency, and the  
4 head of the agency and the inspector general of  
5 the agency that experienced the breach.

6 “(B) CONTENTS.—A report required under  
7 subparagraph (A) shall include a written state-  
8 ment from the entity that delayed the notifica-  
9 tion explaining the need for the delay.

10 “(C) FORM.—The report required under  
11 subparagraph (A) shall be unclassified but may  
12 include a classified annex.

13 “(3) RENEWAL.—A delay under paragraph (1)  
14 shall be for a period of 60 days and may be renewed.

15 “(d) UPDATE NOTIFICATION.—If an agency deter-  
16 mines there is a significant change in the reasonable basis  
17 to conclude that a breach occurred, a significant change  
18 to the determination made under subsection (a)(1), or that  
19 it is necessary to update the details of the information pro-  
20 vided to impacted individuals as described in subsection  
21 (b), the agency shall as expeditiously as practicable and  
22 without unreasonable delay, and in any case not later than  
23 30 days after such a determination, notify each individual  
24 who received a notification pursuant to subsection (a) of  
25 those changes.

1 “(e) EXEMPTION FROM NOTIFICATION.—

2 “(1) IN GENERAL.—The head of an agency, in  
3 consultation with the inspector general of the agen-  
4 cy, may request an exemption from the Director  
5 from complying with the notification requirements  
6 under subsection (a) if the information affected by  
7 the breach is determined by an independent evalua-  
8 tion to be unreadable, including, as appropriate, in-  
9 stances in which the information is—

10 “(A) encrypted; and

11 “(B) determined by the Director of the Cy-  
12 bersecurity and Infrastructure Security Agency  
13 to be of sufficiently low risk of exposure.

14 “(2) APPROVAL.—The Director shall determine  
15 whether to grant an exemption requested under  
16 paragraph (1) in consultation with—

17 “(A) the Director of the Cybersecurity and  
18 Infrastructure Security Agency; and

19 “(B) the Attorney General.

20 “(3) DOCUMENTATION.—Any exemption grant-  
21 ed by the Director under paragraph (1) shall be re-  
22 ported in writing to the head of the agency and the  
23 inspector general of the agency that experienced the  
24 breach and the Director of the Cybersecurity and In-  
25 frastructure Security Agency.

1       “(f) RULE OF CONSTRUCTION.—Nothing in this sec-  
2   tion shall be construed to limit—

3               “(1) the Director from issuing guidance relat-  
4   ing to notifications or the head of an agency from  
5   notifying individuals potentially affected by breaches  
6   that are not determined to be major incidents; or

7               “(2) the Director from issuing guidance relat-  
8   ing to notifications of major incidents or the head of  
9   an agency from providing more information than de-  
10   scribed in subsection (b) when notifying individuals  
11   potentially affected by breaches.

12   **“§ 3593. Congressional and Executive Branch reports**

13       “(a) INITIAL REPORT.—

14               “(1) IN GENERAL.—Not later than 72 hours  
15   after an agency has a reasonable basis to conclude  
16   that a major incident occurred, the head of the  
17   agency impacted by the major incident shall submit  
18   to the appropriate reporting entities a written report  
19   and, to the extent practicable, provide a briefing to  
20   the Committee on Homeland Security and Govern-  
21   mental Affairs of the Senate, the Committee on  
22   Oversight and Reform of the House of Representa-  
23   tives, the Committee on Homeland Security of the  
24   House of Representatives, and the appropriate au-

1       thorization and appropriations committees of Con-  
2       gress, taking into account—

3               “(A) the information known at the time of  
4       the report;

5               “(B) the sensitivity of the details associ-  
6       ated with the major incident; and

7               “(C) the classification level of the informa-  
8       tion contained in the report.

9       “(2) CONTENTS.—A report required under  
10      paragraph (1) shall include, in a manner that ex-  
11      cludes or otherwise reasonably protects personally  
12      identifiable information and to the extent permitted  
13      by applicable law, including privacy and statistical  
14      laws—

15              “(A) a summary of the information avail-  
16      able about the major incident, including how  
17      the major incident occurred, information indi-  
18      cating that the major incident may be a breach,  
19      and information relating to the major incident  
20      as a breach, based on information available to  
21      agency officials as of the date on which the  
22      agency submits the report;

23              “(B) if applicable, a description and any  
24      associated documentation of any circumstances  
25      necessitating a delay in or exemption to notifi-

1 cation to individuals potentially affected by the  
2 major incident under subsection (c) or (e) of  
3 section 3592; and

4 “(C) if applicable, an assessment of the  
5 impacts to the agency, the Federal Government,  
6 or the security of the United States, based on  
7 information available to agency officials on the  
8 date on which the agency submits the report.

9 “(b) SUPPLEMENTAL REPORT.—Within a reasonable  
10 amount of time, but not later than 30 days after the date  
11 on which an agency submits a written report under sub-  
12 section (a), the head of the agency shall provide to the  
13 appropriate reporting entities written updates on the  
14 major incident and, to the extent practicable, provide a  
15 briefing to the congressional committees described in sub-  
16 section (a)(1), including summaries of—

17 “(1) vulnerabilities, means by which the major  
18 incident occurred, and impacts to the agency relat-  
19 ing to the major incident;

20 “(2) any risk assessment and subsequent risk-  
21 based security implementation of the affected infor-  
22 mation system before the date on which the major  
23 incident occurred;

1           “(3) the status of compliance of the affected in-  
2           formation system with applicable security require-  
3           ments at the time of the major incident;

4           “(4) an estimate of the number of individuals  
5           potentially affected by the major incident based on  
6           information available to agency officials as of the  
7           date on which the agency provides the update;

8           “(5) an assessment of the risk of harm to indi-  
9           viduals potentially affected by the major incident  
10          based on information available to agency officials as  
11          of the date on which the agency provides the update;

12          “(6) an update to the assessment of the risk to  
13          agency operations, or to impacts on other agency or  
14          non-Federal entity operations, affected by the major  
15          incident based on information available to agency of-  
16          ficials as of the date on which the agency provides  
17          the update; and

18          “(7) the detection, response, and remediation  
19          actions of the agency, including any support pro-  
20          vided by the Cybersecurity and Infrastructure Secu-  
21          rity Agency under section 3594(d) and status up-  
22          dates on the notification process described in section  
23          3592(a), including any delay or exemption described  
24          in subsection (c) or (e), respectively, of section 3592,  
25          if applicable.

1       “(c) UPDATE REPORT.—If the agency determines  
2 that there is any significant change in the understanding  
3 of the agency of the scope, scale, or consequence of a  
4 major incident for which an agency submitted a written  
5 report under subsection (a), the agency shall provide an  
6 updated report to the appropriate reporting entities that  
7 includes information relating to the change in under-  
8 standing.

9       “(d) ANNUAL REPORT.—Each agency shall submit as  
10 part of the annual report required under section  
11 3554(c)(1) of this title a description of each major inci-  
12 dent that occurred during the 1-year period preceding the  
13 date on which the report is submitted.

14       “(e) DELAY AND EXEMPTION REPORT.—

15               “(1) IN GENERAL.—The Director shall submit  
16 to the appropriate notification entities an annual re-  
17 port on all notification delays and exemptions grant-  
18 ed pursuant to subsections (c) and (d) of section  
19 3592.

20               “(2) COMPONENT OF OTHER REPORT.—The Di-  
21 rector may submit the report required under para-  
22 graph (1) as a component of the annual report sub-  
23 mitted under section 3597(b).



1       “(f) REPORT DELIVERY.—Any written report re-  
2       quired to be submitted under this section may be sub-  
3       mitted in a paper or electronic format.

4       “(g) THREAT BRIEFING.—

5               “(1) IN GENERAL.—Not later than 7 days after  
6       the date on which an agency has a reasonable basis  
7       to conclude that a major incident occurred, the head  
8       of the agency, jointly with the National Cyber Direc-  
9       tor and any other Federal entity determined appro-  
10      priate by the National Cyber Director, shall provide  
11      a briefing to the congressional committees described  
12      in subsection (a)(1) on the threat causing the major  
13      incident.

14              “(2) COMPONENTS.—The briefing required  
15      under paragraph (1)—

16                      “(A) shall, to the greatest extent prac-  
17                      ticable, include an unclassified component; and

18                      “(B) may include a classified component.

19       “(h) RULE OF CONSTRUCTION.—Nothing in this sec-  
20      tion shall be construed to limit—

21                      “(1) the ability of an agency to provide addi-  
22                      tional reports or briefings to Congress; or

23                      “(2) Congress from requesting additional infor-  
24                      mation from agencies through reports, briefings, or  
25                      other means.

1 **“§ 3594. Government information sharing and inci-**  
2 **dent response**

3 “(a) IN GENERAL.—

4 “(1) INCIDENT REPORTING.—The head of each  
5 agency shall provide any information relating to any  
6 incident, whether the information is obtained by the  
7 Federal Government directly or indirectly, to the Cy-  
8 bersecurity and Infrastructure Security Agency and  
9 the Office of Management and Budget.

10 “(2) CONTENTS.—A provision of information  
11 relating to an incident made by the head of an agen-  
12 cy under paragraph (1) shall—

13 “(A) include detailed information about  
14 the safeguards that were in place when the inci-  
15 dent occurred;

16 “(B) whether the agency implemented the  
17 safeguards described in subparagraph (A) cor-  
18 rectly;

19 “(C) in order to protect against a similar  
20 incident, identify—

21 “(i) how the safeguards described in  
22 subparagraph (A) should be implemented  
23 differently; and

24 “(ii) additional necessary safeguards;  
25 and

1 “(D) include information to aid in incident  
2 response, such as—

3 “(i) a description of the affected sys-  
4 tems or networks;

5 “(ii) the estimated dates of when the  
6 incident occurred; and

7 “(iii) information that could reason-  
8 ably help identify the party that conducted  
9 the incident.

10 “(3) INFORMATION SHARING.—To the greatest  
11 extent practicable, the Director of the Cybersecurity  
12 and Infrastructure Security Agency shall share in-  
13 formation relating to an incident with any agencies  
14 that may be impacted by the incident.

15 “(4) NATIONAL SECURITY SYSTEMS.—Each  
16 agency operating or exercising control of a national  
17 security system shall share information about inci-  
18 dents that occur on national security systems with  
19 the Director of the Cybersecurity and Infrastructure  
20 Security Agency to the extent consistent with stand-  
21 ards and guidelines for national security systems  
22 issued in accordance with law and as directed by the  
23 President.

24 “(b) COMPLIANCE.—The information provided under  
25 subsection (a) shall take into account the level of classi-

1 fication of the information and any information sharing  
2 limitations and protections, such as limitations and protec-  
3 tions relating to law enforcement, national security, pri-  
4 vacy, statistical confidentiality, or other factors deter-  
5 mined by the Director

6       “(c) INCIDENT RESPONSE.—Each agency that has a  
7 reasonable basis to conclude that a major incident oc-  
8 curred involving Federal information in electronic medium  
9 or form, as defined by the Director and not involving a  
10 national security system, regardless of delays from notifi-  
11 cation granted for a major incident, shall coordinate with  
12 the Cybersecurity and Infrastructure Security Agency re-  
13 garding—

14               “(1) incident response and recovery; and

15               “(2) recommendations for mitigating future in-  
16 cidents.

17 **“§ 3595. Responsibilities of contractors and awardees**

18       “(a) NOTIFICATION.—

19               “(1) IN GENERAL.—Unless otherwise specified  
20 in a contract, grant, cooperative agreement, or an  
21 other transaction agreement, any contractor or  
22 awardee of an agency shall report to the agency  
23 within the same amount of time such agency is re-  
24 quired to report an incident to the Cybersecurity  
25 and Infrastructure Security Agency, if the con-

1 tractor or awardee has a reasonable basis to con-  
2 clude that—

3 “(A) an incident or breach has occurred  
4 with respect to Federal information collected,  
5 used, or maintained by the contractor or award-  
6 ee in connection with the contract, grant, coop-  
7 erative agreement, or other transaction agree-  
8 ment of the contractor or awardee;

9 “(B) an incident or breach has occurred  
10 with respect to a Federal information system  
11 used or operated by the contractor or awardee  
12 in connection with the contract, grant, coopera-  
13 tive agreement, or other transaction agreement  
14 of the contractor or awardee; or

15 “(C) the contractor or awardee has re-  
16 ceived information from the agency that the  
17 contractor or awardee is not authorized to re-  
18 ceive in connection with the contract, grant, co-  
19 operative agreement, or other transaction agree-  
20 ment of the contractor or awardee.

21 “(2) PROCEDURES.—

22 “(A) MAJOR INCIDENT.—Following a re-  
23 port of a breach or major incident by a con-  
24 tractor or awardee under paragraph (1), the  
25 agency, in consultation with the contractor or

1           awardee, shall carry out the requirements under  
2           sections 3592, 3593, and 3594 with respect to  
3           the major incident.

4           “(B) INCIDENT.—Following a report of an  
5           incident by a contractor or awardee under para-  
6           graph (1), an agency, in consultation with the  
7           contractor or awardee, shall carry out the re-  
8           quirements under section 3594 with respect to  
9           the incident.

10          “(b) EFFECTIVE DATE.—This section shall apply on  
11       and after the date that is 1 year after the date of enact-  
12       ment of the Federal Information Security Modernization  
13       Act of 2021.

14       **“§ 3596. Training**

15          “(a) COVERED INDIVIDUAL DEFINED.—In this sec-  
16       tion, the term ‘covered individual’ means an individual  
17       who obtains access to Federal information or Federal in-  
18       formation systems because of the status of the individual  
19       as an employee, contractor, awardee, volunteer, or intern  
20       of an agency.

21          “(b) REQUIREMENT.—The head of each agency shall  
22       develop training for covered individuals on how to identify  
23       and respond to an incident, including—

24               “(1) the internal process of the agency for re-  
25       porting an incident; and

1           “(2) the obligation of a covered individual to re-  
2       port to the agency a confirmed major incident and  
3       any suspected incident involving information in any  
4       medium or form, including paper, oral, and elec-  
5       tronic.

6       “(c) INCLUSION IN ANNUAL TRAINING.—The train-  
7       ing developed under subsection (b) may be included as  
8       part of an annual privacy or security awareness training  
9       of an agency.

10   **“§ 3597. Analysis and report on Federal incidents**

11       “(a) ANALYSIS OF FEDERAL INCIDENTS.—

12           “(1) QUANTITATIVE AND QUALITATIVE ANAL-  
13       YSES.—The Director of the Cybersecurity and Infra-  
14       structure Security Agency shall develop, in consulta-  
15       tion with the Director and the National Cyber Direc-  
16       tor, and perform continuous monitoring and quan-  
17       titative and qualitative analyses of incidents at agen-  
18       cies, including major incidents, including—

19           “(A) the causes of incidents, including—

20               “(i) attacker tactics, techniques, and  
21               procedures; and

22               “(ii) system vulnerabilities, including  
23               zero days, unpatched systems, and infor-  
24               mation system misconfigurations;

1           “(B) the scope and scale of incidents at  
2 agencies;

3           “(C) cross Federal Government root causes  
4 of incidents at agencies;

5           “(D) agency incident response, recovery,  
6 and remediation actions and the effectiveness of  
7 those actions, as applicable;

8           “(E) lessons learned and recommendations  
9 in responding to, recovering from, remediating,  
10 and mitigating future incidents; and

11           “(F) trends in cross-Federal Government  
12 cybersecurity and incident response capabilities  
13 using the metrics established under section  
14 224(e) of the Cybersecurity Act of 2015 (6  
15 U.S.C. 1522(e)).

16           “(2) AUTOMATED ANALYSIS.—The analyses de-  
17 veloped under paragraph (1) shall, to the greatest  
18 extent practicable, use machine readable data, auto-  
19 mation, and machine learning processes.

20           “(3) SHARING OF DATA AND ANALYSIS.—

21           “(A) IN GENERAL.—The Director shall  
22 share on an ongoing basis the analyses required  
23 under this subsection with agencies and the Na-  
24 tional Cyber Director to—



1                   “(i) improve the understanding of cy-  
2                   bersecurity risk of agencies; and

3                   “(ii) support the cybersecurity im-  
4                   provement efforts of agencies.

5                   “(B) FORMAT.—In carrying out subpara-  
6                   graph (A), the Director shall share the anal-  
7                   yses—

8                   “(i) in human-readable written prod-  
9                   ucts; and

10                  “(ii) to the greatest extent practicable,  
11                  in machine-readable formats in order to  
12                  enable automated intake and use by agen-  
13                  cies.

14                  “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—  
15                  Not later than 2 years after the date of enactment of this  
16                  section, and not less frequently than annually thereafter,  
17                  the Director of the Cybersecurity and Infrastructure Secu-  
18                  rity Agency, in consultation with the Director and other  
19                  Federal agencies as appropriate, shall submit to the ap-  
20                  propriate notification entities a report that includes—

21                  “(1) a summary of causes of incidents from  
22                  across the Federal Government that categorizes  
23                  those incidents as incidents or major incidents;

24                  “(2) the quantitative and qualitative analyses of  
25                  incidents developed under subsection (a)(1) on an

1       agency-by-agency basis and comprehensively across  
2       the Federal Government, including—

3               “(A) a specific analysis of breaches; and

4               “(B) an analysis of the Federal Govern-  
5       ment’s performance against the metrics estab-  
6       lished under section 224(c) of the Cybersecurity  
7       Act of 2015 (6 U.S.C. 1522(c)); and

8       “(3) an annex for each agency that includes—

9               “(A) a description of each major incident;

10              “(B) the total number of compromises of  
11       the agency; and

12              “(C) an analysis of the agency’s perform-  
13       ance against the metrics established under sec-  
14       tion 224(c) of the Cybersecurity Act of 2015 (6  
15       U.S.C. 1522(e)).

16       “(c) PUBLICATION.—A version of each report sub-  
17       mitted under subsection (b) shall be made publicly avail-  
18       able on the website of the Cybersecurity and Infrastruc-  
19       ture Security Agency during the year in which the report  
20       is submitted.

21       “(d) INFORMATION PROVIDED BY AGENCIES.—

22              “(1) IN GENERAL.—The analysis required  
23       under subsection (a) and each report submitted  
24       under subsection (b) shall use information provided  
25       by agencies under section 3594(a).

1           “(2) NONCOMPLIANCE REPORTS.—

2                   “(A) IN GENERAL.—Subject to subpara-  
3 graph (B), during any year during which the  
4 head of an agency does not provide data for an  
5 incident to the Cybersecurity and Infrastructure  
6 Security Agency in accordance with section  
7 3594(a), the head of the agency, in coordina-  
8 tion with the Director of the Cybersecurity and  
9 Infrastructure Security Agency and the Direc-  
10 tor, shall submit to the appropriate reporting  
11 entities a report that includes—

12                           “(i) data for the incident; and

13                           “(ii) the information described in sub-  
14 section (b) with respect to the agency.

15           “(B) EXCEPTION FOR NATIONAL SECURITY  
16 SYSTEMS.—The head of an agency that owns or  
17 exercises control of a national security system  
18 shall not include data for an incident that oc-  
19 curs on a national security system in any report  
20 submitted under subparagraph (A).

21           “(3) NATIONAL SECURITY SYSTEM REPORTS.—

22                   “(A) IN GENERAL.—Annually, the head of  
23 an agency that operates or exercises control of  
24 a national security system shall submit a report  
25 that includes the information described in sub-

1 section (b) with respect to the agency to the ex-  
2 tent that the submission is consistent with  
3 standards and guidelines for national security  
4 systems issued in accordance with law and as  
5 directed by the President to—

6 “(i) the majority and minority leaders  
7 of the Senate,

8 “(ii) the Speaker and minority leader  
9 of the House of Representatives;

10 “(iii) the Committee on Homeland Se-  
11 curity and Governmental Affairs of the  
12 Senate;

13 “(iv) the Select Committee on Intel-  
14 ligence of the Senate;

15 “(v) the Committee on Armed Serv-  
16 ices of the Senate;

17 “(vi) the Committee on Appropria-  
18 tions of the Senate;

19 “(vii) the Committee on Oversight and  
20 Reform of the House of Representatives;

21 “(viii) the Committee on Homeland  
22 Security of the House of Representatives;

23 “(ix) the Permanent Select Committee  
24 on Intelligence of the House of Represent-  
25 atives;

1 “(x) the Committee on Armed Serv-  
2 ices of the House of Representatives; and

3 “(xi) the Committee on Appropria-  
4 tions of the House of Representatives.

5 “(B) CLASSIFIED FORM.—A report re-  
6 quired under subparagraph (A) may be sub-  
7 mitted in a classified form.

8 “(e) REQUIREMENT FOR COMPILING INFORMA-  
9 TION.—In publishing the public report required under  
10 subsection (c), the Director of the Cybersecurity and In-  
11 frastructure Security Agency shall sufficiently compile in-  
12 formation such that no specific incident of an agency can  
13 be identified, except with the concurrence of the Director  
14 of the Office of Management and Budget and in consulta-  
15 tion with the impacted agency.

16 **“§ 3598. Major incident definition**

17 “(a) IN GENERAL.—Not later than 180 days after  
18 the date of enactment of the Federal Information Security  
19 Modernization Act of 2021, the Director, in coordination  
20 with the Director of the Cybersecurity and Infrastructure  
21 Security Agency and the National Cyber Director, shall  
22 develop and promulgate guidance on the definition of the  
23 term ‘major incident’ for the purposes of subchapter II  
24 and this subchapter.

1       “(b) REQUIREMENTS.—With respect to the guidance  
2 issued under subsection (a), the definition of the term  
3 ‘major incident’ shall—

4               “(1) include, with respect to any information  
5 collected or maintained by or on behalf of an agency  
6 or an information system used or operated by an  
7 agency or by a contractor of an agency or another  
8 organization on behalf of an agency—

9               “(A) any incident the head of the agency  
10 determines is likely to have an impact on—

11                       “(i) the national security, homeland  
12 security, or economic security of the  
13 United States; or

14                       “(ii) the civil liberties or public health  
15 and safety of the people of the United  
16 States;

17               “(B) any incident the head of the agency  
18 determines likely to result in an inability for the  
19 agency, a component of the agency, or the Fed-  
20 eral Government, to provide 1 or more critical  
21 services;

22               “(C) any incident that the head of an  
23 agency, in consultation with a senior privacy of-  
24 ficer of the agency, determines is likely to have

1 a significant privacy impact on 1 or more indi-  
2 vidual;

3 “(D) any incident that the head of the  
4 agency, in consultation with a senior privacy of-  
5 ficial of the agency, determines is likely to have  
6 a substantial privacy impact on a significant  
7 number of individuals;

8 “(E) any incident the head of the agency  
9 determines impacts the operations of a high  
10 value asset owned or operated by the agency;

11 “(F) any incident involving the exposure of  
12 sensitive agency information to a foreign entity,  
13 such as the communications of the head of the  
14 agency, the head of a component of the agency,  
15 or the direct reports of the head of the agency  
16 or the head of a component of the agency; and

17 “(G) any other type of incident determined  
18 appropriate by the Director;

19 “(2) stipulate that the National Cyber Director  
20 shall declare a major incident at each agency im-  
21 pacted by an incident if the Director of the Cyberse-  
22 curity and Infrastructure Security Agency deter-  
23 mines that an incident—

24 “(A) occurs at not less than 2 agencies;  
25 and

1           “(B) is enabled by—

2                   “(i) a common technical root cause,  
3                   such as a supply chain compromise, a com-  
4                   mon software or hardware vulnerability; or

5                   “(ii) the related activities of a com-  
6                   mon threat actor; and

7           “(3) stipulate that, in determining whether an  
8           incident constitutes a major incident because that  
9           incident—

10                   “(A) is any incident described in para-  
11                   graph (1), the head of an agency shall consult  
12                   with the Director of the Cybersecurity and In-  
13                   frastructure Security Agency;

14                   “(B) is an incident described in paragraph  
15                   (1)(A), the head of the agency shall consult  
16                   with the National Cyber Director; and

17                   “(C) is an incident described in subpara-  
18                   graph (C) or (D) of paragraph (1), the head of  
19                   the agency shall consult with—

20                   “(i) the Privacy and Civil Liberties  
21                   Oversight Board; and

22                   “(ii) the Chair of the Federal Trade  
23                   Commission.



1       “(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In de-  
2       termining what constitutes a significant number of indi-  
3       viduals under subsection (b)(1)(D), the Director—

4               “(1) may determine a threshold for a minimum  
5       number of individuals that constitutes a significant  
6       amount; and

7               “(2) may not determine a threshold described  
8       in paragraph (1) that exceeds 5,000 individuals.

9       “(d) EVALUATION AND UPDATES.—Not later than 2  
10      years after the date of enactment of the Federal Informa-  
11      tion Security Modernization Act of 2021, and not less fre-  
12      quently than every 2 years thereafter, the Director shall  
13      submit to the Committee on Homeland Security and Gov-  
14      ernmental Affairs of the Senate and the Committee on  
15      Oversight and Reform of the House of Representatives an  
16      evaluation, which shall include—

17              “(1) an update, if necessary, to the guidance  
18      issued under subsection (a);

19              “(2) the definition of the term ‘major incident’  
20      included in the guidance issued under subsection (a);  
21      and

22              “(3) an explanation of, and the analysis that  
23      led to, the definition described in paragraph (2).”.

(2) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding at the end the following:

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification of breach.

“3593. Congressional and Executive Branch reports.

“3594. Government information sharing and incident response.

**“3595. Responsibilities of contractors and awardees.**

“3596. Training.

“3597. Analysis and report on Federal incidents.

“3598. Major incident definition.”.

**4 SEC. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.**

(a) MODERNIZING GOVERNMENT TECHNOLOGY.—  
Subtitle G of title X of Division A of the National Defense  
Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301  
note) is amended—

9 (1) in section 1077(b)—

10 (A) in paragraph (5)(A), by inserting “im-  
11 proving the cybersecurity of systems and” be-  
12 fore “cost savings activities”; and

13 (B) in paragraph (7)—

(i) in the paragraph heading, by striking “CIO” and inserting “CIO”;

16 (ii) by striking “In evaluating  
17 projects” and inserting the following:

18 “(A) CONSIDERATION OF GUIDANCE.—In  
19 evaluating projects”;

20 (iii) in subparagraph (A), as so des-  
21 ignated, by striking “under section

1                   1094(b)(1)” and inserting “by the Direc-  
2                   tor”; and

3                   (iv) by adding at the end the fol-  
4                   lowing:

5                   “(B) CONSULTATION.—In using funds  
6                   under paragraph (3)(A), the Chief Information  
7                   Officer of the covered agency shall consult with  
8                   the necessary stakeholders to ensure the project  
9                   appropriately addresses cybersecurity risks, in-  
10                  cluding the Director of the Cybersecurity and  
11                  Infrastructure Security Agency, as appro-  
12                  priate.”; and

13                  (2) in section 1078—

14                  (A) by striking subsection (a) and insert-  
15                  ing the following:

16                  “(a) DEFINITIONS.—In this section:

17                  “(1) AGENCY.—The term ‘agency’ has the  
18                  meaning given the term in section 551 of title 5,  
19                  United States Code.

20                  “(2) HIGH VALUE ASSET.—The term ‘high  
21                  value asset’ has the meaning given the term in sec-  
22                  tion 3552 of title 44, United States Code.”;

23                  (B) in subsection (b), by adding at the end  
24                  the following:

1           “(8) PROPOSAL EVALUATION.—The Director  
2       shall—

3           “(A) give consideration for the use of  
4       amounts in the Fund to improve the security of  
5       high value assets; and

6           “(B) require that any proposal for the use  
7       of amounts in the Fund includes a cybersecu-  
8       rity plan, including a supply chain risk manage-  
9       ment plan, to be reviewed by the member of the  
10      Technology Modernization Board described in  
11      subsection (c)(5)(C).”; and

12           (C) in subsection (c)—

13           (i) in paragraph (2)(A)(i), by insert-  
14       ing “, including a consideration of the im-  
15       pact on high value assets” after “oper-  
16       ational risks”;

17           (ii) in paragraph (5)—

18           (I) in subparagraph (A), by strik-  
19       ing “and” at the end;

20           (II) in subparagraph (B), by  
21       striking the period at the end and in-  
22       serting “and”; and

23           (III) by adding at the end the  
24       following:



1 (bb) in clause (i), as so des-  
2 ignated, by striking “, and per-  
3 formance” and inserting “secu-  
4 rity, and performance; and”; and  
5 (cc) by adding at the end  
6 the following:

7 “(ii) specifically denote cybersecurity  
8 funding under the risk-based cyber budget  
9 model developed pursuant to section  
10 3553(a)(7) of title 44.”; and

11 (II) in subparagraph (B), adding  
12 at the end the following:

13 “(iii) The Director shall provide to the  
14 National Cyber Director any cybersecurity  
15 funding information described in subpara-  
16 graph (A)(ii) that is provided to the Direc-  
17 tor under clause (ii) of this subpara-  
18 graph.”; and

19 (ii) in paragraph (4)(B), in the matter  
20 preceding clause (i), by inserting “not later  
21 than 30 days after the date on which the  
22 review under subparagraph (A) is com-  
23 pleted,” before “the Administrator”;  
24 (C) in subsection (f)—

1 (i) by striking “heads of executive  
2 agencies to develop” and inserting “heads  
3 of executive agencies to—

4 “(1) develop”;

5 (ii) in paragraph (1), as so des-  
6 ignated, by striking the period at the end  
7 and inserting “; and”; and

8 (iii) by adding at the end the fol-  
9 lowing:

10 “(2) consult with the Director of the Cybersecu-  
11 rity and Infrastructure Security Agency for the de-  
12 velopment and use of supply chain security best  
13 practices.”; and

14 (D) in subsection (h), by inserting “, in-  
15 cluding cybersecurity performances,” after “the  
16 performances”; and

17 (2) in section 11303(b)—

18 (A) in paragraph (2)(B)—

19 (i) in clause (i), by striking “or” at  
20 the end;

21 (ii) in clause (ii), by adding “or” at  
22 the end; and

23 (iii) by adding at the end the fol-  
24 lowing:

1                   “(iii) whether the function should be  
2                   performed by a shared service offered by  
3                   another executive agency;” and

4                   (B) in paragraph (5)(B)(i), by inserting “,  
5                   while taking into account the risk-based cyber  
6                   budget model developed pursuant to section  
7                   3553(a)(7) of title 44” after “title 31”.

8           (c) SUBCHAPTER II.—Subchapter II of subtitle III  
9 of title 40, United States Code, is amended—

10           (1) in section 11312(a), by inserting “, includ-  
11           ing security risks” after “managing the risks”;

12           (2) in section 11313(1), by striking “efficiency  
13           and effectiveness” and inserting “efficiency, security,  
14           and effectiveness”;

15           (3) in section 11315, by adding at the end the  
16           following:

17           “(d) COMPONENT AGENCY CHIEF INFORMATION OF-  
18           FICERS.—The Chief Information Officer or an equivalent  
19           official of a component agency shall report to—

20           “(1) the Chief Information Officer designated  
21           under section 3506(a)(2) of title 44 or an equivalent  
22           official of the agency of which the component agency  
23           is a component; and

24           “(2) the head of the component agency.”;



1 (4) in section 11317, by inserting “security,”  
2 before “or schedule”; and

3 (5) in section 11319(b)(1), in the paragraph  
4 heading, by striking “CIOS” and inserting “CHIEF  
5 INFORMATION OFFICERS”.

6 (d) SUBCHAPTER III.—Section 11331 of title 40,  
7 United States Code, is amended—

8 (1) in subsection (a), by striking “section  
9 3532(b)(1)” and inserting “section 3552(b)”;

10 (2) in subsection (b)(1)(A), by striking “the  
11 Secretary of Homeland Security” and inserting “the  
12 Director of the Cybersecurity and Infrastructure Se-  
13 curity Agency”;

14 (3) by striking subsection (c) and inserting the  
15 following:

16 “(c) APPLICATION OF MORE STRINGENT STAND-  
17 ARDS.—

18 “(1) IN GENERAL.—The head of an agency  
19 shall—

20 “(A) evaluate, in consultation with the sen-  
21 ior agency information security officers, the  
22 need to employ standards for cost-effective,  
23 risk-based information security for all systems,  
24 operations, and assets within or under the su-  
25 pervision of the agency that are more stringent

1           than the standards promulgated by the Director  
2           under this section, if such standards contain, at  
3           a minimum, the provisions of those applicable  
4           standards made compulsory and binding by the  
5           Director; and

6           “(B) to the greatest extent practicable and  
7           if the head of the agency determines that the  
8           standards described in subparagraph (A) are  
9           necessary, employ those standards.

10          “(2) EVALUATION OF MORE STRINGENT STAND-  
11          ARDS.—In evaluating the need to employ more strin-  
12          gent standards under paragraph (1), the head of an  
13          agency shall consider available risk information,  
14          such as—

15               “(A) the status of cybersecurity remedial  
16               actions of the agency;

17               “(B) any vulnerability information relating  
18               to agency systems that is known to the agency;

19               “(C) incident information of the agency;

20               “(D) information from—

21                   “(i) penetration testing performed  
22                   under section 3559A of title 44; and

23                   “(ii) information from the vulner-  
24                   ability disclosure program established  
25                   under section 3559B of title 44;

1           “(E) agency threat hunting results under  
2           section 5145 of the Federal Information Secu-  
3           rity Modernization Act of 2021;

4           “(F) Federal and non-Federal cyber threat  
5           intelligence;

6           “(G) data on compliance with standards  
7           issued under this section;

8           “(H) agency system risk assessments per-  
9           formed under section 3554(a)(1)(A) of title 44;  
10          and

11          “(I) any other information determined rel-  
12          evant by the head of the agency.”;

13          (4) in subsection (d)(2)—

14                (A) in the paragraph heading, by striking  
15                “NOTICE AND COMMENT” and inserting “CON-  
16                SULTATION, NOTICE, AND COMMENT”;

17                (B) by inserting “promulgate,” before  
18                “significantly modify”; and

19                (C) by striking “shall be made after the  
20                public is given an opportunity to comment on  
21                the Director’s proposed decision.” and inserting  
22                “shall be made—

23                “(A) for a decision to significantly modify  
24                or not promulgate such a proposed standard,

1 after the public is given an opportunity to com-  
2 ment on the Director's proposed decision;

3 “(B) in consultation with the Chief Infor-  
4 mation Officers Council, the Director of the Cy-  
5 bersecurity and Infrastructure Security Agency,  
6 the National Cyber Director, the Comptroller  
7 General of the United States, and the Council  
8 of the Inspectors General on Integrity and Effi-  
9 ciency;

10 “(C) considering the Federal risk assess-  
11 ments performed under section 3553(i) of title  
12 44; and

13 “(D) considering the extent to which the  
14 proposed standard reduces risk relative to the  
15 cost of implementation of the standard.”; and  
16 (5) by adding at the end the following:

17 “(e) REVIEW OF OFFICE OF MANAGEMENT AND  
18 BUDGET GUIDANCE AND POLICY.—

19 “(1) CONDUCT OF REVIEW.—

20 “(A) IN GENERAL.—Not less frequently  
21 than once every 3 years, the Director of the Of-  
22 fice of Management and Budget, in consultation  
23 with the Chief Information Officers Council, the  
24 Director of the Cybersecurity and Infrastruc-  
25 ture Security Agency, the National Cyber Di-

1 rector, the Comptroller General of the United  
2 States, and the Council of the Inspectors Gen-  
3 eral on Integrity and Efficiency shall review the  
4 efficacy of the guidance and policy promulgated  
5 by the Director in reducing cybersecurity risks,  
6 including an assessment of the requirements for  
7 agencies to report information to the Director,  
8 and determine whether any changes to that  
9 guidance or policy is appropriate.

10 “(B) FEDERAL RISK ASSESSMENTS.—In  
11 conducting the review described in subpara-  
12 graph (A), the Director shall consider the Fed-  
13 eral risk assessments performed under section  
14 3553(i) of title 44.

15 “(2) UPDATED GUIDANCE.—Not later than 90  
16 days after the date on which a review is completed  
17 under paragraph (1), the Director of the Office of  
18 Management and Budget shall issue updated guid-  
19 ance or policy to agencies determined appropriate by  
20 the Director, based on the results of the review.

21 “(3) PUBLIC REPORT.—Not later than 30 days  
22 after the date on which a review is completed under  
23 paragraph (1), the Director of the Office of Manage-  
24 ment and Budget shall make publicly available a re-  
25 port that includes—

1           “(A) an overview of the guidance and pol-  
2           icy promulgated under this section that is cur-  
3           rently in effect;

4           “(B) the cybersecurity risk mitigation, or  
5           other cybersecurity benefit, offered by each  
6           guidance or policy document described in sub-  
7           paragraph (A); and

8           “(C) a summary of the guidance or policy  
9           to which changes were determined appropriate  
10          during the review and what the changes are an-  
11          ticipated to include.

12          “(4) CONGRESSIONAL BRIEFING.—Not later  
13          than 30 days after the date on which a review is  
14          completed under paragraph (1), the Director shall  
15          provide to the Committee on Homeland Security and  
16          Governmental Affairs of the Senate and the Com-  
17          mittee on Oversight and Reform of the House of  
18          Representatives a briefing on the review.

19          “(f) AUTOMATED STANDARD IMPLEMENTATION  
20          VERIFICATION.—When the Director of the National Insti-  
21          tute of Standards and Technology issues a proposed  
22          standard pursuant to paragraphs (2) and (3) of section  
23          20(a) of the National Institute of Standards and Tech-  
24          nology Act (15 U.S.C. 278g-3(a)), the Director of the Na-  
25          tional Institute of Standards and Technology shall con-

1 sider developing and, if appropriate and practical, develop,  
2 in consultation with the Director of the Cybersecurity and  
3 Infrastructure Security Agency, specifications to enable  
4 the automated verification of the implementation of the  
5 controls within the standard.”.

6 **SEC. 5123. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**  
7 **SPONSE.**

8 (a) **RESPONSIBILITIES OF THE CYBERSECURITY AND**  
9 **INFRASTRUCTURE SECURITY AGENCY.—**

10 (1) **IN GENERAL.**—Not later than 180 days  
11 after the date of enactment of this Act, the Director  
12 of the Cybersecurity and Infrastructure Security  
13 Agency shall—

14 (A) develop a plan for the development of  
15 the analysis required under section 3597(a) of  
16 title 44, United States Code, as added by this  
17 division, and the report required under sub-  
18 section (b) of that section that includes—

19 (i) a description of any challenges the  
20 Director anticipates encountering; and

21 (ii) the use of automation and ma-  
22 chine-readable formats for collecting, com-  
23 piling, monitoring, and analyzing data; and

1 (B) provide to the appropriate congres-  
2 sional committees a briefing on the plan devel-  
3 oped under subparagraph (A).

4 (2) BRIEFING.—Not later than 1 year after the  
5 date of enactment of this Act, the Director of the  
6 Cybersecurity and Infrastructure Security Agency  
7 shall provide to the appropriate congressional com-  
8 mittees a briefing on—

9 (A) the execution of the plan required  
10 under paragraph (1)(A); and

11 (B) the development of the report required  
12 under section 3597(b) of title 44, United States  
13 Code, as added by this division.

14 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE  
15 OFFICE OF MANAGEMENT AND BUDGET.—

16 (1) FISMA.—Section 2 of the Federal Informa-  
17 tion Security Modernization Act of 2014 (44 U.S.C.  
18 3554 note) is amended—

19 (A) by striking subsection (b); and

20 (B) by redesignating subsections (c)  
21 through (f) as subsections (b) through (e), re-  
22 spectively.

23 (2) INCIDENT DATA SHARING.—

24 (A) IN GENERAL.—The Director shall de-  
25 velop guidance, to be updated not less fre-



1           quently than once every 2 years, on the content,  
2           timeliness, and format of the information pro-  
3           vided by agencies under section 3594(a) of title  
4           44, United States Code, as added by this divi-  
5           sion.

6           (B) REQUIREMENTS.—The guidance devel-  
7           oped under subparagraph (A) shall—

8           (i) prioritize the availability of data  
9           necessary to understand and analyze—

10           (I) the causes of incidents;

11           (II) the scope and scale of inci-  
12           dents within the environments and  
13           systems of an agency;

14           (III) a root cause analysis of in-  
15           cidents that—

16           (aa) are common across the  
17           Federal Government; or

18           (bb) have a Government-  
19           wide impact;

20           (IV) agency response, recovery,  
21           and remediation actions and the effec-  
22           tiveness of those actions; and

23           (V) the impact of incidents;

24           (ii) enable the efficient development  
25           of—

1 (I) lessons learned and rec-  
2 ommendations in responding to, recov-  
3 ering from, remediating, and miti-  
4 gating future incidents; and

5 (II) the report on Federal inci-  
6 dents required under section 3597(b)  
7 of title 44, United States Code, as  
8 added by this division;

9 (iii) include requirements for the time-  
10 liness of data production; and

11 (iv) include requirements for using  
12 automation and machine-readable data for  
13 data sharing and availability.

14 (3) GUIDANCE ON RESPONDING TO INFORMA-  
15 TION REQUESTS.—Not later than 1 year after the  
16 date of enactment of this Act, the Director shall de-  
17 velop guidance for agencies to implement the re-  
18 quirement under section 3594(c) of title 44, United  
19 States Code, as added by this division, to provide in-  
20 formation to other agencies experiencing incidents.

21 (4) STANDARD GUIDANCE AND TEMPLATES.—  
22 Not later than 1 year after the date of enactment  
23 of this Act, the Director, in consultation with the  
24 Director of the Cybersecurity and Infrastructure Se-  
25 curity Agency, shall develop guidance and templates,

1 to be reviewed and, if necessary, updated not less  
2 frequently than once every 2 years, for use by Fed-  
3 eral agencies in the activities required under sections  
4 3592, 3593, and 3596 of title 44, United States  
5 Code, as added by this division.

6 (5) CONTRACTOR AND AWARDEE GUIDANCE.—

7 (A) IN GENERAL.—Not later than 1 year  
8 after the date of enactment of this Act, the Di-  
9 rector, in coordination with the Secretary of  
10 Homeland Security, the Secretary of Defense,  
11 the Administrator of General Services, and the  
12 heads of other agencies determined appropriate  
13 by the Director, shall issue guidance to Federal  
14 agencies on how to deconflict, to the greatest  
15 extent practicable, existing regulations, policies,  
16 and procedures relating to the responsibilities of  
17 contractors and awardees established under sec-  
18 tion 3595 of title 44, United States Code, as  
19 added by this division.

20 (B) EXISTING PROCESSES.—To the great-  
21 est extent practicable, the guidance issued  
22 under subparagraph (A) shall allow contractors  
23 and awardees to use existing processes for noti-  
24 fying Federal agencies of incidents involving in-  
25 formation of the Federal Government.

1           (6) UPDATED BRIEFINGS.—Not less frequently  
2           than once every 2 years, the Director shall provide  
3           to the appropriate congressional committees an up-  
4           date on the guidance and templates developed under  
5           paragraphs (2) through (4).

6           (c) UPDATE TO THE PRIVACY ACT OF 1974.—Sec-  
7           tion 552a(b) of title 5, United States Code (commonly  
8           known as the “Privacy Act of 1974”) is amended—

9           (1) in paragraph (11), by striking “or” at the  
10          end;

11          (2) in paragraph (12), by striking the period at  
12          the end and inserting “; or”; and

13          (3) by adding at the end the following:

14          “(13) to another agency in furtherance of a re-  
15          sponse to an incident (as defined in section 3552 of  
16          title 44) and pursuant to the information sharing re-  
17          quirements in section 3594 of title 44 if the head of  
18          the requesting agency has made a written request to  
19          the agency that maintains the record specifying the  
20          particular portion desired and the activity for which  
21          the record is sought.”.

22   **SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**  
23                           **UPDATES.**

24          Not later than 1 year after the date of enactment  
25          of this Act, the Director, in coordination with the Director

1 of the Cybersecurity and Infrastructure Security Agency,  
2 shall issue guidance for agencies on—

3 (1) performing the ongoing and continuous  
4 agency system risk assessment required under sec-  
5 tion 3554(a)(1)(A) of title 44, United States Code,  
6 as amended by this division;

7 (2) implementing additional cybersecurity pro-  
8 cedures, which shall include resources for shared  
9 services;

10 (3) establishing a process for providing the sta-  
11 tus of each remedial action under section 3554(b)(7)  
12 of title 44, United States Code, as amended by this  
13 division, to the Director and the Cybersecurity and  
14 Infrastructure Security Agency using automation  
15 and machine-readable data, as practicable, which  
16 shall include—

17 (A) specific guidance for the use of auto-  
18 mation and machine-readable data; and

19 (B) templates for providing the status of  
20 the remedial action;

21 (4) interpreting the definition of “high value  
22 asset” under section 3552 of title 44, United States  
23 Code, as amended by this division; and

24 (5) a requirement to coordinate with inspectors  
25 general of agencies to ensure consistent under-

1 standing and application of agency policies for the  
2 purpose of evaluations by inspectors general.

3 **SEC. 5125. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**  
4 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

5 (a) DEFINITIONS.—In this section:

6 (1) REPORTING ENTITY.—The term “reporting  
7 entity” means private organization or governmental  
8 unit that is required by statute or regulation to sub-  
9 mit sensitive information to an agency.

10 (2) SENSITIVE INFORMATION.—The term “sen-  
11 sitive information” has the meaning given the term  
12 by the Director in guidance issued under subsection  
13 (b).

14 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-  
15 TITIES.—Not later than 180 days after the date of enact-  
16 ment of this Act, the Director shall issue guidance requir-  
17 ing the head of each agency to notify a reporting entity  
18 of an incident that is likely to substantially affect—

19 (1) the confidentiality or integrity of sensitive  
20 information submitted by the reporting entity to the  
21 agency pursuant to a statutory or regulatory re-  
22 quirement; or

23 (2) the agency information system or systems  
24 used in the transmission or storage of the sensitive  
25 information described in paragraph (1).

**TITLE LII—IMPROVING  
FEDERAL CYBERSECURITY**

**SEC. 5141. MOBILE SECURITY STANDARDS.**

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall—

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

(1) a requirement, pursuant to section 3506(b)(4) of title 44, United States Code, for every agency to maintain a continuous inventory of every—

(A) mobile device operated by or on behalf of the agency; and

(B) vulnerability identified by the agency associated with a mobile device; and

(2) a requirement for every agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(B) and other risks associated with the use of applications on mobile devices.

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and In-

1 frastructure Security Agency, shall issue guidance to  
2 agencies for sharing the inventory of the agency required  
3 under subsection (b)(1) with the Director of the Cyberse-  
4 curity and Infrastructure Security Agency, using automa-  
5 tion and machine-readable data to the greatest extent  
6 practicable.

7 (d) BRIEFING.—Not later than 60 days after the date  
8 on which the Director issues guidance under subsection  
9 (a)(2), the Director, in coordination with the Director of  
10 the Cybersecurity and Infrastructure Security Agency,  
11 shall provide to the appropriate congressional committees  
12 a briefing on the guidance.

13 **SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT**  
14 **RESPONSE.**

15 (a) RECOMMENDATIONS.—Not later than 2 years  
16 after the date of enactment of this Act, and not less fre-  
17 quently than every 2 years thereafter, the Director of the  
18 Cybersecurity and Infrastructure Security Agency, in con-  
19 sultation with the Attorney General, shall submit to the  
20 Director recommendations on requirements for logging  
21 events on agency systems and retaining other relevant  
22 data within the systems and networks of an agency.

23 (b) CONTENTS.—The recommendations provided  
24 under subsection (a) shall include—

25 (1) the types of logs to be maintained;



1           (2) the time periods to retain the logs and other  
2       relevant data;

3           (3) the time periods for agencies to enable rec-  
4       ommended logging and security requirements;

5           (4) how to ensure the confidentiality, integrity,  
6       and availability of logs;

7           (5) requirements to ensure that, upon request,  
8       in a manner that excludes or otherwise reasonably  
9       protects personally identifiable information, and to  
10      the extent permitted by applicable law (including  
11      privacy and statistical laws), agencies provide logs  
12      to—

13                (A) the Director of the Cybersecurity and  
14      Infrastructure Security Agency for a cybersecu-  
15      rity purpose; and

16                (B) the Federal Bureau of Investigation to  
17      investigate potential criminal activity; and

18           (6) requirements to ensure that, subject to com-  
19      pliance with statistical laws and other relevant data  
20      protection requirements, the highest level security  
21      operations center of each agency has visibility into  
22      all agency logs.

23           (c) GUIDANCE.—Not later than 90 days after receiv-  
24      ing the recommendations submitted under subsection (a),  
25      the Director, in consultation with the Director of the Cy-

1 bersecurity and Infrastructure Security Agency and the  
2 Attorney General, shall, as determined to be appropriate  
3 by the Director, update guidance to agencies regarding re-  
4 quirements for logging, log retention, log management,  
5 sharing of log data with other appropriate agencies, or any  
6 other logging activity determined to be appropriate by the  
7 Director.

8 **SEC. 5143. CISA AGENCY ADVISORS.**

9 (a) IN GENERAL.—Not later than 120 days after the  
10 date of enactment of this Act, the Director of the Cyberse-  
11 curity and Infrastructure Security Agency shall assign not  
12 less than 1 cybersecurity professional employed by the Cy-  
13 bersecurity and Infrastructure Security Agency to be the  
14 Cybersecurity and Infrastructure Security Agency advisor  
15 to the senior agency information security officer of each  
16 agency.

17 (b) QUALIFICATIONS.—Each advisor assigned under  
18 subsection (a) shall have knowledge of—

19 (1) cybersecurity threats facing agencies, in-  
20 cluding any specific threats to the assigned agency;

21 (2) performing risk assessments of agency sys-  
22 tems; and

23 (3) other Federal cybersecurity initiatives.

24 (c) DUTIES.—The duties of each advisor assigned  
25 under subsection (a) shall include—

1 (1) providing ongoing assistance and advice, as  
2 requested, to the agency Chief Information Officer;

3 (2) serving as an incident response point of  
4 contact between the assigned agency and the Cyber-  
5 security and Infrastructure Security Agency; and

6 (3) familiarizing themselves with agency sys-  
7 tems, processes, and procedures to better facilitate  
8 support to the agency in responding to incidents.

9 (d) LIMITATION.—An advisor assigned under sub-  
10 section (a) shall not be a contractor.

11 (e) MULTIPLE ASSIGNMENTS.—One individual advi-  
12 sor may be assigned to multiple agency Chief Information  
13 Officers under subsection (a).

14 **SEC. 5144. FEDERAL PENETRATION TESTING POLICY.**

15 (a) IN GENERAL.—Subchapter II of chapter 35 of  
16 title 44, United States Code, is amended by adding at the  
17 end the following:

18 **“§ 3559A. Federal penetration testing**

19 “(a) DEFINITIONS.—In this section:

20 “(1) AGENCY OPERATIONAL PLAN.—The term  
21 ‘agency operational plan’ means a plan of an agency  
22 for the use of penetration testing.

23 “(2) RULES OF ENGAGEMENT.—The term  
24 ‘rules of engagement’ means a set of rules estab-

1       lished by an agency for the use of penetration test-  
2       ing.

3       “(b) GUIDANCE.—

4           “(1) IN GENERAL.—The Director shall issue  
5       guidance that—

6           “(A) requires agencies to use, when and  
7       where appropriate, penetration testing on agen-  
8       cy systems; and

9           “(B) requires agencies to develop an agen-  
10      cy operational plan and rules of engagement  
11      that meet the requirements under subsection  
12      (c).

13       “(2) PENETRATION TESTING GUIDANCE.—The  
14      guidance issued under this section shall—

15           “(A) permit an agency to use, for the pur-  
16      pose of performing penetration testing—

17           “(i) a shared service of the agency or  
18      another agency; or

19           “(ii) an external entity, such as a ven-  
20      dor; and

21           “(B) require agencies to provide the rules  
22      of engagement and results of penetration test-  
23      ing to the Director and the Director of the Cy-  
24      bersecurity and Infrastructure Security Agency,

1 without regard to the status of the entity that  
2 performs the penetration testing.

3 “(c) AGENCY PLANS AND RULES OF ENGAGE-  
4 MENT.—The agency operational plan and rules of engage-  
5 ment of an agency shall—

6 “(1) require the agency to—

7 “(A) perform penetration testing on the  
8 high value assets of the agency; or

9 “(B) coordinate with the Director of the  
10 Cybersecurity and Infrastructure Security  
11 Agency to ensure that penetration testing is  
12 being performed;

13 “(2) establish guidelines for avoiding, as a re-  
14 sult of penetration testing—

15 “(A) adverse impacts to the operations of  
16 the agency;

17 “(B) adverse impacts to operational envi-  
18 ronments and systems of the agency; and

19 “(C) inappropriate access to data;

20 “(3) require the results of penetration testing  
21 to include feedback to improve the cybersecurity of  
22 the agency; and

23 “(4) include mechanisms for providing consist-  
24 ently formatted, and, if applicable, automated and  
25 machine-readable, data to the Director and the Di-

1 rector of the Cybersecurity and Infrastructure Secu-  
2 rity Agency.

3 “(d) RESPONSIBILITIES OF CISA.—The Director of  
4 the Cybersecurity and Infrastructure Security Agency  
5 shall—

6 “(1) establish a process to assess the perform-  
7 ance of penetration testing by both Federal and non-  
8 Federal entities that establishes minimum quality  
9 controls for penetration testing;

10 “(2) develop operational guidance for insti-  
11 tuting penetration testing programs at agencies;

12 “(3) develop and maintain a centralized capa-  
13 bility to offer penetration testing as a service to  
14 Federal and non-Federal entities; and

15 “(4) provide guidance to agencies on the best  
16 use of penetration testing resources.

17 “(e) RESPONSIBILITIES OF OMB.—The Director, in  
18 coordination with the Director of the Cybersecurity and  
19 Infrastructure Security Agency, shall—

20 “(1) not less frequently than annually, inven-  
21 tory all Federal penetration testing assets; and

22 “(2) develop and maintain a standardized proc-  
23 ess for the use of penetration testing.

24 “(f) PRIORITIZATION OF PENETRATION TESTING RE-  
25 SOURCES.—

1           “(1) IN GENERAL.—The Director, in coordina-  
2           tion with the Director of the Cybersecurity and In-  
3           frastructure Security Agency, shall develop a frame-  
4           work for prioritizing Federal penetration testing re-  
5           sources among agencies.

6           “(2) CONSIDERATIONS.—In developing the  
7           framework under this subsection, the Director shall  
8           consider—

9                   “(A) agency system risk assessments per-  
10                  formed under section 3554(a)(1)(A);

11                  “(B) the Federal risk assessment per-  
12                  formed under section 3553(i);

13                  “(C) the analysis of Federal incident data  
14                  performed under section 3597; and

15                  “(D) any other information determined ap-  
16                  propriate by the Director or the Director of the  
17                  Cybersecurity and Infrastructure Security  
18                  Agency.

19           “(g) EXCEPTION FOR NATIONAL SECURITY SYS-  
20           TEMS.—The guidance issued under subsection (b) shall  
21           not apply to national security systems.

22           “(h) DELEGATION OF AUTHORITY FOR CERTAIN  
23           SYSTEMS.—The authorities of the Director described in  
24           subsection (b) shall be delegated—

1 “(1) to the Secretary of Defense in the case of  
2 systems described in section 3553(e)(2); and

3 “(2) to the Director of National Intelligence in  
4 the case of systems described in 3553(e)(3).”.

5 (b) DEADLINE FOR GUIDANCE.—Not later than 180  
6 days after the date of enactment of this Act, the Director  
7 shall issue the guidance required under section 3559A(b)  
8 of title 44, United States Code, as added by subsection  
9 (a).

10 (c) CLERICAL AMENDMENT.—The table of sections  
11 for chapter 35 of title 44, United States Code, is amended  
12 by adding after the item relating to section 3559 the fol-  
13 lowing:

“3559A. Federal penetration testing.”.

14 (d) PENETRATION TESTING BY THE SECRETARY OF  
15 HOMELAND SECURITY.—Section 3553(b) of title 44,  
16 United States Code, as amended by section 5121, is fur-  
17 ther amended—

18 (1) in paragraph (8)(B), by striking “and” at  
19 the end;

20 (2) by redesignating paragraph (9) as para-  
21 graph (10); and

22 (3) by inserting after paragraph (8) the fol-  
23 lowing:

24 “(9) performing penetration testing with or  
25 without advance notice to, or authorization from,



1 agencies, to identify vulnerabilities within Federal  
2 information systems; and”.

3 **SEC. 5145. ONGOING THREAT HUNTING PROGRAM.**

4 (a) **THREAT HUNTING PROGRAM.—**

5 (1) **IN GENERAL.**—Not later than 540 days  
6 after the date of enactment of this Act, the Director  
7 of the Cybersecurity and Infrastructure Security  
8 Agency shall establish a program to provide ongoing,  
9 hypothesis-driven threat-hunting services on the net-  
10 work of each agency.

11 (2) **PLAN.**—Not later than 180 days after the  
12 date of enactment of this Act, the Director of the  
13 Cybersecurity and Infrastructure Security Agency  
14 shall develop a plan to establish the program re-  
15 quired under paragraph (1) that describes how the  
16 Director of the Cybersecurity and Infrastructure Se-  
17 curity Agency plans to—

18 (A) determine the method for collecting,  
19 storing, accessing, and analyzing appropriate  
20 agency data;

21 (B) provide on-premises support to agen-  
22 cies;

23 (C) staff threat hunting services;

24 (D) allocate available human and financial  
25 resources to implement the plan; and

1 (E) provide input to the heads of agencies  
2 on the use of—

3 (i) more stringent standards under  
4 section 11331(c)(1) of title 40, United  
5 States Code; and

6 (ii) additional cybersecurity proce-  
7 dures under section 3554 of title 44,  
8 United States Code.

9 (b) REPORTS.—The Director of the Cybersecurity  
10 and Infrastructure Security Agency shall submit to the ap-  
11 propriate congressional committees—

12 (1) not later than 30 days after the date on  
13 which the Director of the Cybersecurity and Infra-  
14 structure Security Agency completes the plan re-  
15 quired under subsection (a)(2), a report on the plan  
16 to provide threat hunting services to agencies;

17 (2) not less than 30 days before the date on  
18 which the Director of the Cybersecurity and Infra-  
19 structure Security Agency begins providing threat  
20 hunting services under the program under sub-  
21 section (a)(1), a report providing any updates to the  
22 plan developed under subsection (a)(2); and

23 (3) not later than 1 year after the date on  
24 which the Director of the Cybersecurity and Infra-  
25 structure Security Agency begins providing threat

1 hunting services to agencies other than the Cyberse-  
2 curity and Infrastructure Security Agency, a report  
3 describing lessons learned from providing those serv-  
4 ices.

5 **SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PRO-**  
6 **GRAMS.**

7 (a) IN GENERAL.—Chapter 35 of title 44, United  
8 States Code, is amended by inserting after section 3559A,  
9 as added by section 5144 of this division, the following:

10 **“§ 3559B. Federal vulnerability disclosure programs**

11 **“(a) DEFINITIONS.—In this section:**

12 **“(1) REPORT.—The term ‘report’ means a vul-**  
13 **nerability disclosure made to an agency by a re-**  
14 **porter.**

15 **“(2) REPORTER.—The term ‘reporter’ means**  
16 **an individual that submits a vulnerability report**  
17 **pursuant to the vulnerability disclosure process of an**  
18 **agency.**

19 **“(b) RESPONSIBILITIES OF OMB.—**

20 **“(1) LIMITATION ON LEGAL ACTION.—The Di-**  
21 **rector, in consultation with the Attorney General,**  
22 **shall issue guidance to agencies to not recommend or**  
23 **pursue legal action against a reporter or an indi-**  
24 **vidual that conducts a security research activity that**  
25 **the head of the agency determines—**

1           “(A) represents a good faith effort to fol-  
2           low the vulnerability disclosure policy of the  
3           agency developed under subsection (d)(2); and

4           “(B) is authorized under the vulnerability  
5           disclosure policy of the agency developed under  
6           subsection (d)(2).

7           “(2) SHARING INFORMATION WITH CISA.—The  
8           Director, in coordination with the Director of the  
9           Cybersecurity and Infrastructure Security Agency  
10          and in consultation with the National Cyber Direc-  
11          tor, shall issue guidance to agencies on sharing rel-  
12          evant information in a consistent, automated, and  
13          machine readable manner with the Cybersecurity  
14          and Infrastructure Security Agency, including—

15               “(A) any valid or credible reports of newly  
16               discovered or not publicly known vulnerabilities  
17               (including misconfigurations) on Federal infor-  
18               mation systems that use commercial software or  
19               services;

20               “(B) information relating to vulnerability  
21               disclosure, coordination, or remediation activi-  
22               ties of an agency, particularly as those activities  
23               relate to outside organizations—

24                       “(i) with which the head of the agency  
25                       believes the Director of the Cybersecurity

1                   and Infrastructure Security Agency can as-  
2                   sist; or

3                   “(ii) about which the head of the  
4                   agency believes the Director of the Cyber-  
5                   security and Infrastructure Security Agen-  
6                   cy should know; and

7                   “(C) any other information with respect to  
8                   which the head of the agency determines helpful  
9                   or necessary to involve the Cybersecurity and  
10                  Infrastructure Security Agency.

11               “(3) AGENCY VULNERABILITY DISCLOSURE  
12               POLICIES.—The Director shall issue guidance to  
13               agencies on the required minimum scope of agency  
14               systems covered by the vulnerability disclosure policy  
15               of an agency required under subsection (d)(2).

16               “(c) RESPONSIBILITIES OF CISA.—The Director of  
17               the Cybersecurity and Infrastructure Security Agency  
18               shall—

19               “(1) provide support to agencies with respect to  
20               the implementation of the requirements of this sec-  
21               tion;

22               “(2) develop tools, processes, and other mecha-  
23               nisms determined appropriate to offer agencies capa-  
24               bilities to implement the requirements of this sec-  
25               tion; and

1           “(3) upon a request by an agency, assist the  
2           agency in the disclosure to vendors of newly identi-  
3           fied vulnerabilities in vendor products and services.

4           “(d) RESPONSIBILITIES OF AGENCIES.—

5           “(1) PUBLIC INFORMATION.—The head of each  
6           agency shall make publicly available, with respect to  
7           each internet domain under the control of the agen-  
8           cy that is not a national security system—

9                   “(A) an appropriate security contact; and

10                   “(B) the component of the agency that is  
11           responsible for the internet accessible services  
12           offered at the domain.

13           “(2) VULNERABILITY DISCLOSURE POLICY.—

14           The head of each agency shall develop and make  
15           publicly available a vulnerability disclosure policy for  
16           the agency, which shall—

17                   “(A) describe—

18                           “(i) the scope of the systems of the  
19                           agency included in the vulnerability disclo-  
20                           sure policy;

21                           “(ii) the type of information system  
22                           testing that is authorized by the agency;

23                           “(iii) the type of information system  
24                           testing that is not authorized by the agen-  
25                           cy; and

1                   “(iv) the disclosure policy of the agen-  
2                   cy for sensitive information;

3                   “(B) with respect to a report to an agency,  
4                   describe—

5                   “(i) how the reporter should submit  
6                   the report; and

7                   “(ii) if the report is not anonymous,  
8                   when the reporter should anticipate an ac-  
9                   knowledgment of receipt of the report by  
10                  the agency;

11                  “(C) include any other relevant informa-  
12                  tion; and

13                  “(D) be mature in scope, to cover all Fed-  
14                  eral information systems used or operated by  
15                  that agency or on behalf of that agency.

16                  “(3) IDENTIFIED VULNERABILITIES.—The head  
17                  of each agency shall incorporate any vulnerabilities  
18                  reported under paragraph (2) into the vulnerability  
19                  management process of the agency in order to track  
20                  and remediate the vulnerability.

21                  “(e) PAPERWORK REDUCTION ACT EXEMPTION.—  
22                  The requirements of subchapter I (commonly known as  
23                  the ‘Paperwork Reduction Act’) shall not apply to a vul-  
24                  nerability disclosure program established under this sec-  
25                  tion.

1       “(f) CONGRESSIONAL REPORTING.—Not later than  
2 90 days after the date of enactment of the Federal Infor-  
3 mation Security Modernization Act of 2021, and annually  
4 thereafter for a 3-year period, the Director shall provide  
5 to the Committee on Homeland Security and Govern-  
6 mental Affairs of the Senate and the Committee on Over-  
7 sight and Reform of the House of Representatives a brief-  
8 ing on the status of the use of vulnerability disclosure poli-  
9 cies under this section at agencies, including, with respect  
10 to the guidance issued under subsection (b)(3), an identi-  
11 fication of the agencies that are compliant and not compli-  
12 ant.

13       “(g) EXEMPTIONS.—The authorities and functions of  
14 the Director and Director of the Cybersecurity and Infra-  
15 structure Security Agency under this section shall not  
16 apply to national security systems.

17       “(h) DELEGATION OF AUTHORITY FOR CERTAIN  
18 SYSTEMS.—The authorities of the Director and the Direc-  
19 tor of the Cybersecurity and Infrastructure Security Agen-  
20 cy described in this section shall be delegated—

21               “(1) to the Secretary of Defense in the case of  
22 systems described in section 3553(e)(2); and

23               “(2) to the Director of National Intelligence in  
24 the case of systems described in section  
25 3553(e)(3).”.



1 (b) CLERICAL AMENDMENT.—The table of sections  
2 for chapter 35 of title 44, United States Code, is amended  
3 by adding after the item relating to section 3559A, as  
4 added by section 204, the following:

“3559B. Federal vulnerability disclosure programs.”.

5 **SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE**  
6 **AND LEAST PRIVILEGE PRINCIPLES.**

7 (a) GUIDANCE.—Not later than 1 year after the date  
8 of enactment of this Act, the Director shall provide an  
9 update to the appropriate congressional committees on  
10 progress in increasing the internal defenses of agency sys-  
11 tems, including—

12 (1) shifting away from “trusted networks” to  
13 implement security controls based on a presumption  
14 of compromise;

15 (2) implementing principles of least privilege in  
16 administering information security programs;

17 (3) limiting the ability of entities that cause in-  
18 cidents to move laterally through or between agency  
19 systems;

20 (4) identifying incidents quickly;

21 (5) isolating and removing unauthorized entities  
22 from agency systems quickly;

23 (6) otherwise increasing the resource costs for  
24 entities that cause incidents to be successful; and

1 (7) a summary of the agency progress reports  
2 required under subsection (b).

3 (b) AGENCY PROGRESS REPORTS.—Not later than 1  
4 year after the date of enactment of this Act, the head of  
5 each agency shall submit to the Director a progress report  
6 on implementing an information security program based  
7 on the presumption of compromise and least privilege  
8 principles, which shall include—

9 (1) a description of any steps the agency has  
10 completed, including progress toward achieving re-  
11 quirements issued by the Director;

12 (2) an identification of activities that have not  
13 yet been completed and that would have the most  
14 immediate security impact; and

15 (3) a schedule to implement any planned activi-  
16 ties.

17 **SEC. 5148. AUTOMATION REPORTS.**

18 (a) OMB REPORT.—Not later than 180 days after  
19 the date of enactment of this Act, the Director shall sub-  
20 mit to the appropriate congressional committees a report  
21 on the use of automation under paragraphs (1), (5)(C)  
22 and (8)(B) of section 3554(b) of title 44, United States  
23 Code.

24 (b) GAO REPORT.—Not later than 1 year after the  
25 date of enactment of this Act, the Comptroller General

1 of the United States shall perform a study on the use of  
2 automation and machine readable data across the Federal  
3 Government for cybersecurity purposes, including the  
4 automated updating of cybersecurity tools, sensors, or  
5 processes by agencies.

6 **SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECU-**  
7 **RITY COUNCIL.**

8 Section 1328 of title 41, United States Code, is  
9 amended by striking “the date that” and all that follows  
10 and inserting “December 31, 2026.”.

11 **SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON IN-**  
12 **TEGRITY AND EFFICIENCY DASHBOARD.**

13 (a) **DASHBOARD REQUIRED.**—Section 11(e)(2) of the  
14 Inspector General Act of 1978 (5 U.S.C. App.) is amend-  
15 ed—

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

18 (2) by redesignating subparagraph (B) as sub-  
19 paragraph (C); and

20 (3) by inserting after subparagraph (A) the fol-  
21 lowing:

22 “(B) that shall include a dashboard of  
23 open information security recommendations  
24 identified in the independent evaluations re-

1           quired by section 3555(a) of title 44, United  
2           States Code; and”.

3 **SEC. 5151. QUANTITATIVE CYBERSECURITY METRICS.**

4       (a) **DEFINITION OF COVERED METRICS.**—In this sec-  
5       tion, the term “covered metrics” means the metrics estab-  
6       lished, reviewed, and updated under section 224(c) of the  
7       Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

8       (b) **UPDATING AND ESTABLISHING METRICS.**—Not  
9       later than 1 year after the date of enactment of this Act,  
10      the Director of the Cybersecurity and Infrastructure Secu-  
11      rity Agency, in coordination with the Director, shall—

12           (1) evaluate any covered metrics established as  
13           of the date of enactment of this Act; and

14           (2) as appropriate and pursuant to section  
15           224(c) of the Cybersecurity Act of 2015 (6 U.S.C.  
16           1522(c))—

17                   (A) update the covered metrics; and

18                   (B) establish new covered metrics.

19       (c) **IMPLEMENTATION.**—

20           (1) **IN GENERAL.**—Not later than 540 days  
21           after the date of enactment of this Act, the Director,  
22           in coordination with the Director of the Cybersecu-  
23           rity and Infrastructure Security Agency, shall pro-  
24           mulgate guidance that requires each agency to use

1 covered metrics to track trends in the cybersecurity  
2 and incident response capabilities of the agency.

3 (2) PERFORMANCE DEMONSTRATION.—The  
4 guidance issued under paragraph (1) and any subse-  
5 quent guidance shall require agencies to share with  
6 the Director of the Cybersecurity and Infrastructure  
7 Security Agency data demonstrating the perform-  
8 ance of the agency using the covered metrics in-  
9 cluded in the guidance.

10 (3) PENETRATION TESTS.—On not less than 2  
11 occasions during the 2-year period following the date  
12 on which guidance is promulgated under paragraph  
13 (1), the Director shall ensure that not less than 3  
14 agencies are subjected to substantially similar pene-  
15 tration tests, as determined by the Director, in co-  
16 ordination with the Director of the Cybersecurity  
17 and Infrastructure Security Agency, in order to vali-  
18 date the utility of the covered metrics.

19 (4) ANALYSIS CAPACITY.—The Director of the  
20 Cybersecurity and Infrastructure Security Agency  
21 shall develop a capability that allows for the analysis  
22 of the covered metrics, including cross-agency per-  
23 formance of agency cybersecurity and incident re-  
24 sponse capability trends.

25 (d) CONGRESSIONAL REPORTS.—

1           (1) UTILITY OF METRICS.—Not later than 1  
2       year after the date of enactment of this Act, the Di-  
3       rector of the Cybersecurity and Infrastructure Secu-  
4       rity Agency shall submit to the appropriate congres-  
5       sional committees a report on the utility of the cov-  
6       ered metrics.

7           (2) USE OF METRICS.—Not later than 180 days  
8       after the date on which the Director promulgates  
9       guidance under subsection (c)(1), the Director shall  
10      submit to the appropriate congressional committees  
11      a report on the results of the use of the covered  
12      metrics by agencies.

13       (e) CYBERSECURITY ACT OF 2015 UPDATES.—Sec-  
14      tion 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522)  
15      is amended—

16           (1) by striking subsection (c) and inserting the  
17      following:

18      “(c) IMPROVED METRICS.—

19           “(1) IN GENERAL.—The Director of the Cyber-  
20      security and Infrastructure Security Agency, in co-  
21      ordination with the Director, shall establish, review,  
22      and update metrics to measure the cybersecurity and  
23      incident response capabilities of agencies in accord-  
24      ance with the responsibilities of agencies under sec-  
25      tion 3554 of title 44, United States Code.

1           “(2) QUALITIES.—With respect to the metrics  
2           established, reviewed, and updated under paragraph  
3           (1)—

4                   “(A) not less than 2 of the metrics shall be  
5           time-based, such as a metric of—

6                           “(i) the amount of time it takes for  
7                           an agency to detect an incident; and

8                           “(ii) the amount of time that passes  
9                           between—

10                               “(I) the detection of an incident  
11                               and the remediation of the incident;  
12                               and

13                               “(II) the remediation of an inci-  
14                               dent and the recovery from the inci-  
15                               dent; and

16                           “(B) the metrics may include other meas-  
17                           urable outcomes.”;

18                           (2) by striking subsection (e); and

19                           (3) by redesignating subsection (f) as sub-  
20                           section (e).

21                   **TITLE LIII—RISK-BASED**  
22                   **BUDGET MODEL**

23           **SEC. 5161. DEFINITIONS.**

24           In this title:

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 cyber threat intelligence, incident  
8 data, and tactics, techniques, procedures, and  
9 capabilities of cyber threats; and

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

13 **SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET**  
14 **MODEL.**

15 (a) IN GENERAL.—

16 (1) MODEL.—Not later than 1 year after the  
17 first publication of the budget submitted by the  
18 President under section 1105 of title 31, United  
19 States Code, following the date of enactment of this  
20 Act, the Director, in consultation with the Director  
21 of the Cybersecurity and Infrastructure Security  
22 Agency and the National Cyber Director and in co-  
23 ordination with the Director of the National Insti-  
24 tute of Standards and Technology, shall develop a

1 standard model for creating a risk-based budget for  
2 cybersecurity spending.

3 (2) RESPONSIBILITY OF DIRECTOR.—Section  
4 3553(a) of title 44, United States Code, as amended  
5 by section 5121 of this division, is further amended  
6 by inserting after paragraph (6) the following:

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

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

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

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

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

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

1 (i) information technology and cyber-  
2 security tools;

3 (ii) information technology and cyber-  
4 security architectures;

5 (iii) information technology and cyber-  
6 security personnel; and

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

9 (E) be used to evaluate and inform Gov-  
10 ernment-wide cybersecurity programs of the De-  
11 partment of Homeland Security.

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

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

21 (6) REPORTS.—Not later than 1 year after the  
22 date of enactment of this Act, and annually there-  
23 after for each of the 2 following fiscal years or until  
24 the date on which the model required to be devel-  
25 oped under this subsection is completed, whichever is

1       sooner, the Director shall submit a report to Con-  
2       gress on the development of the model.

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

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

11          (2) AGENCY PERFORMANCE PLANS.—Section  
12      3554(d)(2) of title 44, United States Code, is  
13      amended by inserting “and the risk-based budget  
14      model required under section 3553(a)(7)” after  
15      “paragraph (1)”.

16      (c) VERIFICATION.—

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

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

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

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

1 “(V) a validation that the budg-  
2 ets submitted were developed using a  
3 risk-based methodology; and

4 “(VI) a report on the progress of  
5 each agency on closing recommenda-  
6 tions identified under the independent  
7 evaluation required by section  
8 3555(a)(1) of title 44.”.

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) REPORTS.—

14 (1) INDEPENDENT EVALUATION.—Section  
15 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, as amended by section 5121, is  
5           further amended by inserting after paragraph (5)  
6           the following:

7           “(6) an assessment of—

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

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

12           “(C) whether the model mitigates the  
13           cyber vulnerabilities of the Federal Govern-  
14           ment.”.

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

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

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

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

8 (4) any other information relating to risk-based  
9 budgets the Comptroller General determines appro-  
10 priate.

11 **TITLE LIV—PILOT PROGRAMS**  
12 **TO ENHANCE FEDERAL CY-**  
13 **BERSECURITY**

14 **SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.**

15 (a) DEFINITION.—In this section, the term “active  
16 defense technique”—

17 (1) means an action taken on the systems of an  
18 entity to increase the security of information on the  
19 network of an agency by misleading an adversary;  
20 and

21 (2) includes a honeypot, deception, or purpose-  
22 fully feeding false or misleading data to an adver-  
23 sary when the adversary is on the systems of the en-  
24 tity.

1 (b) STUDY.—Not later than 180 days after the date  
2 of enactment of this Act, the Director of the Cybersecurity  
3 and Infrastructure Security Agency, in coordination with  
4 the Director, shall perform a study on the use of active  
5 defense techniques to enhance the security of agencies,  
6 which shall include—

7 (1) a review of legal restrictions on the use of  
8 different active cyber defense techniques in Federal  
9 environments, in consultation with the Department  
10 of Justice;

11 (2) an evaluation of—

12 (A) the efficacy of a selection of active de-  
13 fense techniques determined by the Director of  
14 the Cybersecurity and Infrastructure Security  
15 Agency; and

16 (B) factors that impact the efficacy of the  
17 active defense techniques evaluated under sub-  
18 paragraph (A);

19 (3) recommendations on safeguards and proce-  
20 dures that shall be established to require that active  
21 defense techniques are adequately coordinated to en-  
22 sure that active defense techniques do not impede  
23 threat response efforts, criminal investigations, and  
24 national security activities, including intelligence col-  
25 lection; and