

117TH CONGRESS  
2D SESSION

# H. R. 6497

To modernize Federal information security management and improve Federal cybersecurity to combat persisting and emerging threats, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

JANUARY 25, 2022

Mrs. CAROLYN B. MALONEY of New York (for herself, Mr. COMER, Mr. CONNOLLY, Mr. SESSIONS, Ms. NORTON, Mr. KELLER, Ms. WASSERMAN SCHULTZ, Mr. HICE of Georgia, Mr. COOPER, Mr. C. SCOTT FRANKLIN of Florida, Ms. BROWN of Ohio, Mr. GIBBS, Mr. LYNCH, and Mr. RASKIN) introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

## A BILL

To modernize Federal information security management and improve Federal cybersecurity to combat persisting and emerging threats, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Information  
5 Security Modernization Act of 2022”.

**1 SEC. 2. TABLE OF CONTENTS.**

2 The table of contents for this Act is as follows:

- 3 Sec. 1. Short title.
- 4 Sec. 2. Table of contents.
- 5 Sec. 3. Definitions.

TITLE I—UPDATES TO FISMA

- 6 Sec. 101. Title 44 amendments.
- 7 Sec. 102. Amendments to subtitle III of title 40.
- 8 Sec. 103. Actions to enhance Federal incident response.
- 9 Sec. 104. Additional guidance to agencies on FISMA updates.
- 10 Sec. 105. Agency requirements to notify private sector entities impacted by incidents.

TITLE II—IMPROVING FEDERAL CYBERSECURITY

- 11 Sec. 201. Mobile security standards.
- 12 Sec. 202. Data and logging retention for incident response.
- 13 Sec. 203. Federal penetration testing policy.
- 14 Sec. 204. Ongoing threat hunting program.
- 15 Sec. 205. Codifying vulnerability disclosure programs.
- 16 Sec. 206. Implementing zero trust architecture.
- 17 Sec. 207. GAO automation report.
- 18 Sec. 208. Extension of Federal Acquisition Security Council.
- 19 Sec. 209. Federal chief information security officer.
- 20 Sec. 210. Extension of Chief Data Officer Council.
- 21 Sec. 211. Council of the inspectors general on integrity and efficiency dashboard.
- 22 Sec. 212. Quantitative cybersecurity metrics.

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL  
CYBERSECURITY

- 23 Sec. 301. Risk-based budget pilot.
- 24 Sec. 302. Active cyber defensive study.
- 25 Sec. 303. Security operations center as a service pilot.
- 26 Sec. 304. Endpoint detection and response as a service pilot.

**3 SEC. 3. DEFINITIONS.**

4 In this Act, unless otherwise specified:

- 5 (1) **ADDITIONAL CYBERSECURITY PROCEDURE.**—The term “additional cybersecurity procedure” has the meaning given the term in section
- 6
- 7
- 8 3552(b) of title 44, United States Code, as amended
- 9 by this Act.

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

4           (3) APPROPRIATE CONGRESSIONAL COMMIT-  
5 TEES.—The term “appropriate congressional com-  
6 mittees” means—

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

9                   (B) the Committee on Oversight and Re-  
10 form of the House of Representatives; and

11                   (C) the Committee on Homeland Security  
12 of the House of Representatives.

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

16           (5) INCIDENT.—The term “incident” has the  
17 meaning given the term in section 3552(b) of title  
18 44, United States Code.

19           (6) NATIONAL SECURITY SYSTEM.—The term  
20 “national security system” has the meaning given  
21 the term in section 3552(b) of title 44, United  
22 States Code.

23           (7) PENETRATION TEST.—The term “penetra-  
24 tion test” has the meaning given the term in section

1 3552(b) of title 44, United States Code, as amended  
2 by this Act.

3 (8) THREAT HUNTING.—The term “threat  
4 hunting” means iteratively searching systems for  
5 threats that evade detection by automated threat de-  
6 tection systems.

7 (9) ZERO TRUST ARCHITECTURE.—The term  
8 “zero trust architecture” means a security model, a  
9 set of system design principles, and a coordinated  
10 cybersecurity and system management strategy that  
11 employs continuous monitoring, risk-based access  
12 controls, or system security automation techniques  
13 to address the cybersecurity principle that threats  
14 exist both inside and outside traditional network  
15 boundaries with an assumption that a breach is in-  
16 evitable or has likely already occurred, and therefore  
17 employs least-privileged access for network or system  
18 users while monitoring for anomalous or malicious  
19 activity.

## 20 **TITLE I—UPDATES TO FISMA**

### 21 **SEC. 101. TITLE 44 AMENDMENTS.**

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

24 (1) in subsection (a)(1)(B) of section 3504—

1 (A) by striking clause (v) and inserting the  
2 following:

3 “(v) confidentiality, privacy, dislo-  
4 sure, and sharing of information;”;

5 (B) by redesignating clause (vi) as clause  
6 (vii); and

7 (C) by inserting after clause (v) the fol-  
8 lowing:

9 “(vi) in consultation with the National  
10 Cyber Director, confidentiality and security  
11 of information; and”;

12 (2) in section 3505—

13 (A) in paragraph (2) of the first subsection  
14 designated as subsection (c) by adding “dis-  
15 covery of internet-accessible information sys-  
16 tems and assets, as well as” after “an inventory  
17 under this subsection shall include”;

18 (B) in paragraph (3) of the first subsection  
19 designated as subsection (c)—

20 (i) in subparagraph (B)—

21 (I) by inserting “the Secretary of  
22 Homeland Security acting through the  
23 Director of the Cybersecurity and In-  
24 frastructure Security Agency, the Na-

1                    tional Cyber Director, and” before  
2                    “the Comptroller General”; and

3                    (II) by striking “and” at the end;

4                    (ii) in subparagraph (C)(v), by strik-  
5                    ing the period at the end and inserting “;  
6                    and”; and

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

9                    “(D) maintained on a continual basis  
10                   through the use of automation, machine-read-  
11                   able data, and scanning wherever practicable.”;  
12                   and

13                   (C) by striking the second subsection des-  
14                   igned as subsection (e);

15                   (3) in section 3506—

16                   (A) in subsection (a)(3), by inserting “In  
17                   carrying out these duties, the Chief Information  
18                   Officer shall coordinate, as appropriate, with  
19                   the Chief Data Officer in accordance with the  
20                   designated functions under section 3520(e).”  
21                   after “reduction of information collection bur-  
22                   dens on the public.”; and

23                   (B) in subsection (b)(1)(C), by inserting “,  
24                   availability” after “integrity”; and

25                   (4) in section 3513—

1 (A) by redesignating subsection (c) as sub-  
2 section (d); and

3 (B) by inserting after subsection (b) the  
4 following:

5 “(c) Each agency providing a written plan under sub-  
6 section (b) shall provide any portion of the written plan  
7 addressing information security to the National Cyber Di-  
8 rector.”.

9 (b) SUBCHAPTER II DEFINITIONS.—

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

12 (A) by redesignating paragraphs (1), (2),  
13 (3), (4), (5), (6), and (7) as paragraphs (2),  
14 (4), (5), (6), (7), (9), and (11), respectively;

15 (B) by inserting before paragraph (2), as  
16 so redesignated, the following:

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

23 (C) by inserting after paragraph (2), as so  
24 redesignated, the following:

1           “(3) The term ‘high value asset’ means infor-  
2           mation or an information system that the head of an  
3           agency determines, using policies, principles, stand-  
4           ards, or guidelines issued by the Director under sec-  
5           tion 3553(a), to be so critical to the agency that the  
6           loss or corruption of the information or the loss of  
7           access to the information system would have a seri-  
8           ous impact on the ability of the agency to perform  
9           the mission of the agency or conduct business.”;

10                   (D) by inserting after paragraph (7), as so  
11                   redesignated, the following:

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

15                   (E) by inserting after paragraph (9), as so  
16                   redesignated, the following:

17           “(10) The term ‘penetration test’ has the mean-  
18           ing given the term in guidance issued by the Direc-  
19           tor.”; and

20                   (F) by inserting after paragraph (11), as  
21                   so redesignated, the following:

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



1 (2) CONFORMING AMENDMENTS.—

2 (A) HOMELAND SECURITY ACT OF 2002.—  
3 Section 1001(c)(1)(A) of the Homeland Secu-  
4 rity Act of 2002 (6 U.S.C. 511(1)(A)) is  
5 amended by striking “section 3552(b)(5)” and  
6 inserting “section 3552(b)”.

7 (B) TITLE 10.—

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

12 (ii) SECTION 2223.—Section  
13 2223(c)(3) of title 10, United States Code,  
14 is amended by striking “section  
15 3552(b)(6)” and inserting “section  
16 3552(b)”.

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

21 (iv) SECTION 2339A.—Section  
22 2339a(e)(5) of title 10, United States  
23 Code, is amended by striking “section  
24 3552(b)(6)” and inserting “section  
25 3552(b)”.

1 (C) HIGH-PERFORMANCE COMPUTING ACT  
2 OF 1991.—Section 207(a) of the High-Perform-  
3 ance Computing Act of 1991 (15 U.S.C.  
4 5527(a)) is amended by striking “section  
5 3552(b)(6)(A)(i)” and inserting “section  
6 3552(b)(9)(A)(i)”.

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

13 (E) NATIONAL DEFENSE AUTHORIZATION  
14 ACT FOR FISCAL YEAR 2013.—Section  
15 933(e)(1)(B) of the National Defense Author-  
16 ization Act for Fiscal Year 2013 (10 U.S.C.  
17 2224 note) is amended by striking “section  
18 3542(b)(2)” and inserting “section 3552(b)”.

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

1 (i) in section 806(e)(5) (10 U.S.C.  
2 2304 note), by striking “section 3542(b)”  
3 and inserting “section 3552(b)”;

4 (ii) in section 931(b)(3) (10 U.S.C.  
5 2223 note), by striking “section  
6 3542(b)(2)” and inserting “section  
7 3552(b)”;

8 (iii) in section 932(b)(2) (10 U.S.C.  
9 2224 note), by striking “section  
10 3542(b)(2)” and inserting “section  
11 3552(b)”.

12 (G) E-GOVERNMENT ACT OF 2002.—Sec-  
13 tion 301(c)(1)(A) of the E-Government Act of  
14 2002 (44 U.S.C. 3501 note) is amended by  
15 striking “section 3542(b)(2)” and inserting  
16 “section 3552(b)”.

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

21 (i) in subsection (a)(2), by striking  
22 “section 3552(b)(5)” and inserting “sec-  
23 tion 3552(b)”;

24 (ii) in subsection (f)—

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

4 (II) in paragraph (5), by striking  
5 “section 3532(b)(2)” and inserting  
6 “section 3552(b)”.

7 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II  
8 of chapter 35 of title 44, United States Code, is amend-  
9 ed—

10 (1) in section 3551—

11 (A) in paragraph (4), by striking “diag-  
12 nose and improve” and inserting “integrate, de-  
13 liver, diagnose, and improve”;

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

16 (C) in paragraph (6), by striking the pe-  
17 riod at the end and inserting a semicolon; and

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

19 “(7) recognize that each agency has specific  
20 mission requirements and, at times, unique cyberse-  
21 curity requirements to meet the mission of the agen-  
22 cy;

23 “(8) recognize that each agency does not have  
24 the same resources to secure agency systems, and an  
25 agency should not be expected to have the capability

1 to secure the systems of the agency from advanced  
2 adversaries alone; and

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

6 (2) in section 3553—

7 (A) in subsection (a)—

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

10 (ii) in paragraph (6), by striking the  
11 period at the end and inserting “; and”;  
12 and

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

15 “(7) promoting, in consultation with the Direc-  
16 tor of the Cybersecurity and Infrastructure Security  
17 Agency, the National Cyber Director, and the Direc-  
18 tor of the National Institute of Standards and Tech-  
19 nology—

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

1           “(B) the use of zero trust architecture to  
2 improve resiliency and timely response actions  
3 to incidents on Federal systems.”;

4           (B) in subsection (b)—

5           (i) in the matter preceding paragraph  
6 (1), by striking “The Secretary, in con-  
7 sultation with the Director” and inserting  
8 “The Secretary of Homeland Security, act-  
9 ing through the Director of the Cybersecu-  
10 rity and Infrastructure Security Agency  
11 and in consultation with the Director and  
12 the National Cyber Director”;

13           (ii) in paragraph (2)(A), by inserting  
14 “and reporting requirements under sub-  
15 chapter IV of this chapter” after “section  
16 3556”;

17           (iii) redesignate paragraphs (8) and  
18 (9) as paragraphs (9) and (10); and

19           (iv) insert a new paragraph (8):

20           “(8) expeditiously seek opportunities to reduce  
21 costs, administrative burdens, and other barriers to  
22 information technology security and modernization  
23 for Federal agencies, including through—

24           “(A) central shared services contracts for  
25 cybersecurity capabilities identified as optimal

1 by the Director, in coordination with the Sec-  
2 retary acting through the Director of the Cy-  
3 bersecurity and Infrastructure Security Agency  
4 and other agencies as appropriate; and

5 “(B) offering technical assistance and ex-  
6 pertise to agencies on the selection and success-  
7 ful engagement of highly adaptive cybersecurity  
8 service contracts and other relevant contracts  
9 provided by the U.S. General Services Adminis-  
10 tration.”;

11 (C) in subsection (c)—

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

18 (ii) by striking paragraph (1);

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

22 (iv) in paragraph (3), as so redesign-  
23 ated, by striking “and” at the end; and

24 (v) by inserting after paragraph (3),  
25 as so redesignated, the following:

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

3           (D) by redesignating subsections (i), (j),  
4 (k), and (l) as subsections (j), (k), (l), and (m)  
5 respectively;

6           (E) in subsection (h)—

7           (i) in paragraph (2), subparagraph  
8 (A) adding “and the National Cyber Direc-  
9 tor” after “in coordination with the Direc-  
10 tor”;

11           (ii) in paragraph (2), subparagraph  
12 (D) adding “, the National Cyber Direc-  
13 tor,” after “notify the Director”; and

14           (iii) in paragraph (3), subparagraph  
15 (A), clause (iv) adding “, the National  
16 Cyber Director,” after “the Secretary pro-  
17 vides prior notice to the Director”;

18           (F) by inserting after subsection (h) the  
19 following:

20           “(i) FEDERAL RISK ASSESSMENTS.—On an ongoing  
21 and continuous basis, the Director of the Cybersecurity  
22 and Infrastructure Security Agency shall perform assess-  
23 ments using any available information on the cybersecu-  
24 rity posture of agencies, and brief the Director and Na-



1 tional Cyber Director on the findings of those assessments  
2 including—

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

5 “(2) any vulnerability information relating to  
6 the systems of an agency that is known by the agen-  
7 cy;

8 “(3) analysis of incident information under sec-  
9 tion 3597;

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

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

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

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

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

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

22 “(10) any other information the Director of the  
23 Cybersecurity and Infrastructure Security Agency  
24 determines relevant.”;

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

1 (i) by striking “Not later than” and  
2 inserting:

3 “(1) IN GENERAL.—Not later than”;

4 (ii) by striking “regarding the spe-  
5 cific” and inserting “that includes a sum-  
6 mary of—

7 “(A) the specific”;

8 (iii) in paragraph (1), as so des-  
9 ignated, by striking the period at the end  
10 and inserting “; and”; and

11 (iv) by adding at the end the fol-  
12 lowing:

13 “(B) the trends identified in the Federal  
14 risk assessments performed under subsection  
15 (i).

16 “(2) FORM.—The report required under para-  
17 graph (1) shall be unclassified but may include a  
18 classified annex.”; and

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

20 “(n) BINDING OPERATIONAL DIRECTIVES.—If the  
21 Director of the Cybersecurity and Infrastructure Security  
22 Agency issues a binding operational directive or an emer-  
23 gency directive under this section, not later than 7 days  
24 after the date on which the binding operational directive  
25 requires an agency to take an action, the Director of the

1 Cybersecurity and Infrastructure Security Agency shall  
2 provide to the Director and National Cyber Director the  
3 status of the implementation of the binding operational  
4 directive at the agency.”;

5 (3) in section 3554—

6 (A) in subsection (a)—

7 (i) in paragraph (1)—

8 (I) by redesignating subpara-  
9 graphs (A), (B), and (C) as subpara-  
10 graphs (B), (C), and (D), respectively;

11 (II) by inserting before subpara-  
12 graph (B), as so redesignated, the fol-  
13 lowing:

14 “(A) on an ongoing and continuous basis,  
15 performing an agency system risk assessment  
16 that—

17 “(i) identifies and documents the high  
18 value assets of the agency using guidance  
19 from the Director;

20 “(ii) evaluates the data assets inven-  
21 toried under section 3511 for sensitivity to  
22 compromises in confidentiality, integrity,  
23 and availability;

1           “(iii) identifies agency systems that  
2           have access to or hold the data assets  
3           inventoried under section 3511;

4           “(iv) evaluates the threats facing  
5           agency systems and data, including high  
6           value assets, based on Federal and non-  
7           Federal cyber threat intelligence products,  
8           where available;

9           “(v) evaluates the vulnerability of  
10          agency systems and data, including high  
11          value assets, including by analyzing—

12                 “(I) the results of penetration  
13                 testing performed by the Department  
14                 of Homeland Security under section  
15                 3553(b)(9);

16                 “(II) the results of penetration  
17                 testing performed under section  
18                 3559A;

19                 “(III) information provided to  
20                 the agency through the vulnerability  
21                 disclosure program of the agency  
22                 under section 3559B;

23                 “(IV) incidents; and

1                   “(V) any other vulnerability in-  
2                   formation relating to agency systems  
3                   that is known to the agency;

4                   “(vi) assesses the impacts of potential  
5                   agency incidents to agency systems, data,  
6                   and operations based on the evaluations  
7                   described in clauses (ii) and (iv) and the  
8                   agency systems identified under clause  
9                   (iii); and

10                  “(vii) assesses the consequences of po-  
11                  tential incidents occurring on agency sys-  
12                  tems that would impact systems at other  
13                  agencies, including due to interconnectivity  
14                  between different agency systems or oper-  
15                  ational reliance on the operations of the  
16                  system or data in the system;”;

17                  (III) in subparagraph (B), as so  
18                  redesignated, in the matter preceding  
19                  clause (i), by striking “providing in-  
20                  formation” and inserting “using infor-  
21                  mation from the assessment con-  
22                  ducted under subparagraph (A), pro-  
23                  viding information”;

24                  (IV) in subparagraph (C), as so  
25                  redesignated—

1 (aa) in clause (ii) by insert-  
2 ing “binding” before “oper-  
3 ational”; and

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

6 (V) by adding at the end the fol-  
7 lowing:

8 “(E) providing an update on the ongoing  
9 and continuous assessment performed under  
10 subparagraph (A)—

11 “(i) upon request, to the inspector  
12 general of the agency or the Comptroller  
13 General of the United States; and

14 “(ii) on a periodic basis, as deter-  
15 mined by guidance issued by the Director  
16 but not less frequently than every 2 years,  
17 to—

18 “(I) the Director;

19 “(II) the Director of the Cyberse-  
20 curity and Infrastructure Security  
21 Agency; and

22 “(III) the National Cyber Direc-  
23 tor;

24 “(F) in consultation with the Director of  
25 the Cybersecurity and Infrastructure Security

1 Agency and not less frequently than once every  
2 3 years, performing an evaluation of whether  
3 additional cybersecurity procedures are appro-  
4 priate for securing a system of, or under the  
5 supervision of, the agency, which shall—

6 “(i) be completed considering the  
7 agency system risk assessment performed  
8 under subparagraph (A); and

9 “(ii) include a specific evaluation for  
10 high value assets;

11 “(G) not later than 30 days after com-  
12 pleting the evaluation performed under sub-  
13 paragraph (F), providing the evaluation and an  
14 implementation plan, if applicable, for using ad-  
15 ditional cybersecurity procedures determined to  
16 be appropriate to—

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

19 “(ii) the Director; and

20 “(iii) the National Cyber Director;

21 and

22 “(H) if the head of the agency determines  
23 there is need for additional cybersecurity proce-  
24 dures, ensuring that those additional cybersecu-

1 rity procedures are reflected in the budget re-  
2 quest of the agency;” and

3 (ii) in paragraph (2)—

4 (I) in subparagraph (A), by in-  
5 serting “in accordance with the agen-  
6 cy system risk assessment performed  
7 under paragraph (1)(A)” after “infor-  
8 mation systems”;

9 (II) in subparagraph (B)—

10 (aa) by striking “in accord-  
11 ance with standards” and insert-  
12 ing “in accordance with—

13 “(i) standards”; and

14 (bb) by adding at the end  
15 the following:

16 “(ii) the evaluation performed under  
17 paragraph (1)(F); and

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

20 (III) in subparagraph (D), by in-  
21 serting “, through the use of penetra-  
22 tion testing, the vulnerability disclo-  
23 sure program established under sec-  
24 tion 3559B, and other means,” after  
25 “periodically”;



1 (B) in subsection (b)—

2 (i) by striking paragraph (1) and in-  
3 sserting the following:

4 “(1) pursuant to subsection (a)(1)(A), per-  
5 forming ongoing and continuous agency system risk  
6 assessment, which may include using automated  
7 tools consistent with standards and guidelines pro-  
8 mulgated under section 11331 of title 40, as applica-  
9 ble;”;

10 (ii) in paragraph (2)(D)—

11 (I) by redesignating clauses (iii)  
12 and (iv) as clauses (iv) and (v), re-  
13 spectively;

14 (II) by inserting after clause (ii)  
15 the following:

16 “(iii) binding operational directives  
17 and emergency directives promulgated by  
18 the Director of the Cybersecurity and In-  
19 frastructure Security Agency under section  
20 3553;” and

21 (III) in clause (iv), as so redesi-  
22 gnated, by striking “as determined by  
23 the agency; and” and inserting “as  
24 determined by the agency, considering

1 the agency risk assessment performed  
2 under subsection (a)(1)(A).”;

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

6 (iv) by redesignating paragraphs (7)  
7 and (8) as paragraphs (8) and (9), respec-  
8 tively;

9 (v) by inserting after paragraph (6)  
10 the following:

11 “(7) a process for providing the status of every  
12 remedial action, as well as unremediated identified  
13 system vulnerabilities, to the Director and the Direc-  
14 tor of the Cybersecurity and Infrastructure Security  
15 Agency, using automation and machine-readable  
16 data to the greatest extent practicable;” and

17 (vi) in paragraph (8)(C), as so redesi-  
18 gnated—

19 (I) by striking clause (ii) and in-  
20 serting the following:

21 “(ii) notifying and consulting with the  
22 Federal information security incident cen-  
23 ter established under section 3556 pursu-  
24 ant to the requirements of section 3594;”;

1 (II) by redesignating clause (iii)  
2 as clause (iv);

3 (III) by inserting after clause (ii)  
4 the following:

5 “(iii) performing the notifications and  
6 other activities required under subchapter  
7 IV of this chapter; and”;

8 (IV) in clause (iv), as so redesign-  
9 nated—

10 (aa) in subclause (II), by  
11 adding “and” at the end;

12 (bb) by striking subclause  
13 (III); and

14 (cc) by redesignating sub-  
15 clause (IV) as subclause (III);  
16 and

17 (C) in subsection (c)—

18 (i) by redesignating paragraph (2) as  
19 paragraph (5);

20 (ii) by striking paragraph (1) and in-  
21 serting the following:

22 “(1) BIENNIAL REPORT.—Not later than 2  
23 years after the date of the enactment of the Federal  
24 Information Security Modernization Act of 2022 and  
25 not less frequently than once every 2 years there-

1 after, using the continuous and ongoing agency sys-  
2 tem risk assessment under subsection (a)(1)(A), the  
3 head of each agency shall submit to the Director,  
4 the Director of the Cybersecurity and Infrastructure  
5 Security Agency, the majority and minority leaders  
6 of the Senate, the Speaker and minority leader of  
7 the House of Representatives, the Committee on  
8 Homeland Security and Governmental Affairs of the  
9 Senate, the Committee on Oversight and Reform of  
10 the House of Representatives, the Committee on  
11 Homeland Security of the House of Representatives,  
12 the Committee on Commerce, Science, and Trans-  
13 portation of the Senate, the Committee on Science,  
14 Space, and Technology of the House of Representa-  
15 tives, the appropriate authorization and appropria-  
16 tions committees of Congress, the National Cyber  
17 Director, and the Comptroller General of the United  
18 States a report that—

19 “(A) summarizes the agency system risk  
20 assessment performed under subsection  
21 (a)(1)(A);

22 “(B) evaluates the adequacy and effective-  
23 ness of information security policies, proce-  
24 dures, and practices of the agency to address  
25 the risks identified in the agency system risk

1 assessment performed under subsection  
2 (a)(1)(A), including an analysis of the agency’s  
3 cybersecurity and incident response capabilities  
4 using the metrics established under section  
5 224(c) of the Cybersecurity Act of 2015 (6  
6 U.S.C. 1522(c));

7 “(C) summarizes the evaluation and imple-  
8 mentation plans described in subparagraphs (F)  
9 and (G) of subsection (a)(1) and whether those  
10 evaluation and implementation plans call for  
11 the use of additional cybersecurity procedures  
12 determined to be appropriate by the agency;  
13 and

14 “(D) summarizes the status of remedial  
15 actions identified by inspector general of the  
16 agency, the Comptroller General of the United  
17 States, and any other source determined appro-  
18 priate by the head of the agency.

19 “(2) UNCLASSIFIED REPORTS.—Each report  
20 submitted under paragraph (1)—

21 “(A) shall be, to the greatest extent prac-  
22 ticable, in an unclassified and otherwise uncon-  
23 trolled form; and

24 “(B) may include a classified annex.

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

6           “(4) BRIEFINGS.—During each year during  
7           which a report is not required to be submitted under  
8           paragraph (1), the Director shall provide to the con-  
9           gressional committees described in paragraph (1) a  
10          briefing summarizing current cybersecurity posture  
11          of agencies.”; and

12                         (iii) in paragraph (5), as so redesign-  
13                         ated, by inserting “, including the report-  
14                         ing procedures established under section  
15                         11315(d) of title 40 and subsection  
16                         (a)(3)(A)(v) of this section,” after “poli-  
17                         cies, procedures, and practices”; and

18          (4) in section 3555—

19                         (A) in the section heading, by striking  
20                         “**ANNUAL INDEPENDENT**” and inserting  
21                         “**INDEPENDENT**”;

22                         (B) in subsection (a)—

23                                 (i) in paragraph (1), by inserting  
24                                 “during which a report is required to be

1 submitted under section 3553(c),” after  
2 “Each year”;

3 (ii) in paragraph (2)(A), by inserting  
4 “, including by penetration testing and  
5 analyzing the vulnerability disclosure pro-  
6 gram of the agency” after “information  
7 systems”; and

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

10 “(3) An evaluation under this section may in-  
11 clude recommendations for improving the cybersecu-  
12 rity posture of the agency.”;

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

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

18 (E) by striking subsection (f) and inserting  
19 the following:

20 “(f) PROTECTION OF INFORMATION.—(1) Agencies,  
21 evaluators, and other recipients of information that, if dis-  
22 closed, may cause grave harm to the efforts of Federal  
23 information security officers, shall take appropriate steps  
24 to ensure the protection of that information, including  
25 safeguarding the information from public disclosure.

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

4       “(3) With respect to information that is not related  
5 to national security systems, agencies and evaluators shall  
6 make a summary of the information unclassified and pub-  
7 licly available, including information that does not iden-  
8 tify—

9               “(A) specific information system incidents; or

10              “(B) specific information system  
11 vulnerabilities.”;

12              (F) in subsection (g)(2)—

13                      (i) by striking “this subsection shall”  
14 and inserting “this subsection—

15                      “(A) shall”;

16                      (ii) in subparagraph (A), as so des-  
17 igned, by striking the period at the end  
18 and inserting “; and”; and

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

21                      “(B) identify any entity that performs an  
22 independent evaluation under subsection (b).”;

23 and

24              (G) striking subsection (j); and



1 (5) in section 3556(a)(4) by striking “3554(b)”  
2 and inserting “3554(a)(1)(A)”.

3 (d) CONFORMING AMENDMENTS.—

4 (1) TABLE OF SECTIONS.—The table of sections  
5 for chapter 35 of title 44, United States Code, is  
6 amended—

7 (A) by striking the item relating to section  
8 3553 and inserting the following:

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

9 and

10 (B) by striking the item relating to section  
11 3555 and inserting the following:

“3555. Independent evaluation.”.

12 (2) OMB REPORTS.—Section 226(e) of the Cy-  
13 bersecurity Act of 2015 (6 U.S.C. 1524(e)) is  
14 amended—

15 (A) in paragraph (1)(B), in the matter  
16 preceding clause (i), by striking “annually  
17 thereafter” and inserting “thereafter during the  
18 years during which a report is required to be  
19 submitted under section 3553(c) of title 44,  
20 United States Code”; and

21 (B) in paragraph (2)(B), in the matter  
22 preceding clause (i)—

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

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

9 (3) NIST RESPONSIBILITIES.—Section  
10 20(d)(3)(B) of the National Institute of Standards  
11 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is  
12 amended by striking “annual”.

13 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

17 “SUBCHAPTER IV—FEDERAL SYSTEM  
18 INCIDENT RESPONSE

19 **“§ 3591. Definitions**

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

23 “(b) ADDITIONAL DEFINITIONS.—As used in this  
24 subchapter:

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

3           “(A) the majority and minority leaders of  
4 the Senate;

5           “(B) the Speaker and minority leader of  
6 the House of Representatives;

7           “(C) the Committee on Homeland Security  
8 and Governmental Affairs of the Senate;

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

11           “(E) the Committee on Homeland Security  
12 of the House of Representatives;

13           “(F) the appropriate authorization and ap-  
14 propriations committees of Congress;

15           “(G) the Director;

16           “(H) the Director of the Cybersecurity and  
17 Infrastructure Security Agency;

18           “(I) the National Cyber Director;

19           “(J) the Comptroller General of the United  
20 States; and

21           “(K) the inspector general of any impacted  
22 agency.

23           “(2) AWARDEE.—The term ‘awardee’—

24           “(A) means a person, business, or other  
25 entity that receives a grant from, or is a party

1 to a cooperative agreement or an other trans-  
2 action agreement with, an agency; and

3 “(B) includes any subgrantee of a person,  
4 business, or other entity described in subpara-  
5 graph (A).

6 “(3) BREACH.—The term ‘breach’ shall be de-  
7 fined by the Director.

8 “(4) CONTRACTOR.—The term ‘contractor’  
9 means a prime contractor of an agency or a subcon-  
10 tractor of a prime contractor of an agency.

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

16 “(6) FEDERAL INFORMATION SYSTEM.—The  
17 term ‘Federal information system’ means an infor-  
18 mation system used or operated by an agency, a con-  
19 tractor, or another organization on behalf of an  
20 agency.

21 “(7) INTELLIGENCE COMMUNITY.—The term  
22 ‘intelligence community’ has the meaning given the  
23 term in section 3 of the National Security Act of  
24 1947 (50 U.S.C. 3003).

1           “(8) NATIONWIDE CONSUMER REPORTING  
2 AGENCY.—The term ‘nationwide consumer reporting  
3 agency’ means a consumer reporting agency de-  
4 scribed in section 603(p) of the Fair Credit Report-  
5 ing Act (15 U.S.C. 1681a(p)).

6           “(9) VULNERABILITY DISCLOSURE.—The term  
7 ‘vulnerability disclosure’ means a vulnerability iden-  
8 tified under section 3559B.

9 **“§ 3592. Notification of breach**

10          “(a) NOTIFICATION.—As expeditiously as practicable  
11 and without unreasonable delay, and in any case not later  
12 than 45 days after an agency has a reasonable basis to  
13 conclude that a breach has occurred, the head of the agen-  
14 cy, in consultation with the chief privacy officer of the  
15 agency, shall—

16           “(1) determine whether notice to any individual  
17 potentially affected by the breach is appropriate  
18 based on an assessment of the risk of harm to the  
19 individual that considers—

20                   “(A) the nature and sensitivity of the per-  
21 sonally identifiable information affected by the  
22 breach;

23                   “(B) the likelihood of access to and use of  
24 the personally identifiable information affected  
25 by the breach;

1           “(C) the type of breach; and

2           “(D) any other factors determined by the  
3           Director; and

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

7           “(A) to the last known mailing address of  
8           the individual; or

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

14          “(b) CONTENTS OF NOTICE.—Each notice of a  
15          breach provided to an individual under subsection (a)(2)  
16          shall include—

17                 “(1) a brief description of the breach;

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

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

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

1           “(B) may include a telephone number,  
2           mailing address, or a website;

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

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

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

14          “(c) DELAY OF NOTIFICATION.—

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

19                         “(A) impede a criminal investigation or a  
20                         national security activity;

21                         “(B) reveal sensitive sources and methods;

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

23                         “(D) hamper security remediation actions.

24          “(2) DOCUMENTATION.—

1           “(A) IN GENERAL.—Any delay under para-  
2 graph (1) shall be reported in writing to the Di-  
3 rector, the Attorney General, the Director of  
4 National Intelligence, the Secretary of Home-  
5 land Security, the National Cyber Director, the  
6 Director of the Cybersecurity and Infrastruc-  
7 ture Security Agency, and the head of the agen-  
8 cy and the inspector general of the agency that  
9 experienced the breach.

10           “(B) CONTENTS.—A report required under  
11 subparagraph (A) shall include a written state-  
12 ment from the entity that delayed the notifica-  
13 tion explaining the need for the delay.

14           “(C) FORM.—The report required under  
15 subparagraph (A) shall be unclassified but may  
16 include a classified annex.

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

19           “(d) UPDATE NOTIFICATION.—If an agency deter-  
20 mines there is a significant change in the reasonable basis  
21 to conclude that a breach occurred, a significant change  
22 to the determination made under subsection (a)(1), or that  
23 it is necessary to update the details of the information pro-  
24 vided to potentially affected individuals as described in  
25 subsection (b), the agency shall as expeditiously as prac-



1 ticable and without unreasonable delay, and in any case  
2 not later than 30 days after such a determination, notify  
3 each individual who received a notification pursuant to  
4 subsection (a) of those changes.

5 “(e) RULE OF CONSTRUCTION.—Nothing in this sec-  
6 tion shall be construed to limit—

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

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

16 **“§ 3593. Congressional and executive branch reports**

17 “(a) INITIAL REPORT.—

18 “(1) IN GENERAL.—Not later than 72 hours  
19 after an agency has a reasonable basis to conclude  
20 that a major incident occurred, the head of the  
21 agency impacted by the major incident shall submit  
22 to the appropriate reporting entities a written re-  
23 port. Within 7 days of a major incident determina-  
24 tion, the head of the agency impacted shall coordi-  
25 nate with the National Cyber Director, or their des-

1       ignee, to provide a briefing, along with any other  
2       Federal entity determined appropriate by the Na-  
3       tional Cyber Director, to the Committee on Home-  
4       land Security and Governmental Affairs of the Sen-  
5       ate, the Committee on Oversight and Reform of the  
6       House of Representatives, the Committee on Home-  
7       land Security of the House of Representatives, and  
8       the appropriate authorization and appropriations  
9       committees of Congress, in the manner requested by  
10      the Congressional entities, taking into account—

11               “(A) the information known at the time of  
12               the report, including the threat having likely  
13               caused the major incident;

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

16               “(C) the classification level of the informa-  
17               tion contained in the report.

18               “(2) CONTENTS.—A report required under  
19               paragraph (1) shall include, in a manner that ex-  
20               cludes or otherwise reasonably protects personally  
21               identifiable information and to the extent permitted  
22               by applicable law, including privacy and statistical  
23               laws—

24                       “(A) a summary of the information avail-  
25                       able about the major incident, including how

1 the major incident occurred and, if applicable,  
2 information relating to the major incident as a  
3 breach, based on information available to agen-  
4 cy officials as of the date on which the agency  
5 submits the report;

6 “(B) if applicable, whether any ransom has  
7 been demanded or paid, or plans to be paid, by  
8 any entity operating a Federal information sys-  
9 tem or with access to a Federal information  
10 system, unless disclosure of such information  
11 may disrupt an active Federal law enforcement  
12 or national security operation;

13 “(C) if applicable, a description and any  
14 associated documentation of any circumstances  
15 necessitating a delay in notification to individ-  
16 uals potentially affected by the major incident  
17 under subsection (c) of section 3592; and

18 “(D) if applicable, an assessment of the  
19 impacts to the agency, the Federal Government,  
20 or the security of the United States, based on  
21 information available to agency officials on the  
22 date on which the agency submits the report.

23 “(3) COMPONENTS OF BRIEFING.—The 7 day  
24 briefing required under paragraph (1)—

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

3           “(B) may include a classified component.

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

12           “(1) vulnerabilities, means by which the major  
13 incident occurred, and impacts to the agency relat-  
14 ing to the major incident;

15           “(2) any risk assessment and subsequent risk-  
16 based security implementation of the affected infor-  
17 mation system before the date on which the major  
18 incident occurred;

19           “(3) an estimate of the number of individuals  
20 potentially affected by the major incident based on  
21 information available to agency officials as of the  
22 date on which the agency provides the update;

23           “(4) an assessment of the risk of harm to indi-  
24 viduals potentially affected by the major incident

1 based on information available to agency officials as  
2 of the date on which the agency provides the update;

3 “(5) an update to the assessment of the risk to  
4 agency operations, or to impacts on other agency or  
5 non-Federal entity operations, affected by the major  
6 incident based on information available to agency of-  
7 ficials as of the date on which the agency provides  
8 the update; and

9 “(6) the detection, response, and remediation  
10 actions of the agency, including any support pro-  
11 vided by the Cybersecurity and Infrastructure Secu-  
12 rity Agency under section 3594(d) and status up-  
13 dates on the notification process described in section  
14 3592(a), including any delay described in subsection  
15 (c) of section 3592, if applicable.

16 “(c) UPDATE REPORT.—If the agency, or the Na-  
17 tional Cyber Director, determines that there is any signifi-  
18 cant change in the understanding of the agency of the  
19 scope, scale, or consequence of a major incident for which  
20 an agency submitted a written report under subsection  
21 (a), the agency shall provide an updated report to the ap-  
22 propriate reporting entities that includes information re-  
23 lating to the change in understanding.

24 “(d) BIENNIAL REPORT.—Each agency shall submit  
25 as part of the biannual report required under section

1 3554(c)(1) of this title a description of each major inci-  
2 dent that occurred during the 2-year period preceding the  
3 date on which the biannual report is submitted.

4 “(e) DELAY REPORT.—

5 “(1) IN GENERAL.—The Director shall submit  
6 to the appropriate reporting entities an annual re-  
7 port on all notification delays granted pursuant to  
8 subsection (c) of section 3592.

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

13 “(f) REPORT AND BRIEFING CONSISTENCY.—In car-  
14 rying out the duties under this section, and to achieve con-  
15 sistent and understandable agency reporting to Congress,  
16 the National Cyber Director shall—

17 “(1) provide to agencies formatting guidelines  
18 and recommended contents of information to be in-  
19 cluded in the reports and briefings required under  
20 this section, including recommendations for the use  
21 of plain language terminology and consistent for-  
22 mats for presenting any associated metrics; and

23 “(2) maintain a historical archive and major in-  
24 cident log of all reports and briefings provided under  
25 the requirements of this section, which shall include

1 at a minimum an archive of the full contents of any  
2 written report and associated documentation, the re-  
3 porting agency, the date of submission, and a list of  
4 the recipient Congressional entities, which shall be  
5 made available upon request to the Congressional  
6 entities listed under subsection (a)(1) and may, to  
7 the extent practicable, utilize an internet accessible  
8 portal for appropriate Congressional staff to directly  
9 access the log and archived materials required to be  
10 maintained under this paragraph.

11 “(g) REPORT DELIVERY.—Any written report re-  
12 quired to be submitted under this section may be sub-  
13 mitted in a paper or electronic format.

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

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

18 “(2) Congress from requesting additional infor-  
19 mation from agencies through reports, briefings, or  
20 other means.

21 **“§ 3594. Government information sharing and inci-**  
22 **dent response**

23 “(a) IN GENERAL.—

24 “(1) INCIDENT REPORTING.—Subject to limita-  
25 tions in subsection (b), the head of each agency shall

1 provide the information described in paragraph (2)  
2 relating to an incident affecting the agency, whether  
3 the information is obtained by the Federal Govern-  
4 ment directly or indirectly, to the Cybersecurity and  
5 Infrastructure Security Agency, the Office of Man-  
6 agement and Budget, and the Office of the National  
7 Cyber Director in a manner specified by the Director  
8 under subsection (b).

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

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

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

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

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

23 “(ii) additional necessary safeguards;  
24 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, as appropriate.

10           “(3) INFORMATION SHARING.—To the greatest  
11 extent practicable, the Director of the Cybersecurity  
12 and Infrastructure Security Agency shall—

13           “(A) share information relating to an inci-  
14 dent with any agencies that may be impacted  
15 by the incident, or are potentially susceptible or  
16 similarly targeted, as well as with appropriate  
17 Federal law enforcement agencies to facilitate  
18 any necessary threat response activities as re-  
19 quested; and

20           “(B) coordinate, in consultation with the  
21 National Cyber Director, any necessary infor-  
22 mation sharing efforts related to a major inci-  
23 dent with the private sector.

24           “(4) NATIONAL SECURITY SYSTEMS.—Each  
25 agency operating or exercising control of a national

1 security system shall share information about inci-  
2 dents that occur on national security systems with  
3 the Director of the Cybersecurity and Infrastructure  
4 Security Agency to the extent consistent with stand-  
5 ards and guidelines for national security systems  
6 issued in accordance with law and as directed by the  
7 President.

8 “(b) COMPLIANCE.—The information provided and  
9 method of reporting under subsection (a) shall take into  
10 account the level of classification of the information and  
11 any information sharing limitations and protections, such  
12 as limitations and protections relating to law enforcement,  
13 national security, privacy, statistical confidentiality, or  
14 other factors determined by the Director in order to imple-  
15 ment subsection (a)(1) in a manner that enables auto-  
16 mated and consistent reporting.

17 “(c) INCIDENT RESPONSE.—Each agency that has a  
18 reasonable basis to conclude that a major incident oc-  
19 curred involving Federal information in electronic medium  
20 or form, as defined by the Director and not involving a  
21 national security system, regardless of delays from notifi-  
22 cation granted for a major incident, shall coordinate with  
23 the Cybersecurity and Infrastructure Security Agency to  
24 facilitate asset response activities and recommendations  
25 for mitigating future incidents, and with appropriate Fed-

1 eral law enforcement agencies to facilitate threat response  
2 activities, consistent with relevant policies, principles,  
3 standards, and guidelines on information security.

4 **“§ 3595. Responsibilities of contractors and awardees**

5 “(a) REPORTING.—

6 “(1) IN GENERAL.—Unless otherwise specified  
7 in a contract, grant, cooperative agreement, or any  
8 other transaction agreement, any contractor or  
9 awardee of an agency shall report to the agency  
10 within the same amount of time such agency is re-  
11 quired to report an incident to the Cybersecurity  
12 and Infrastructure Security Agency, if the con-  
13 tractor or awardee has a reasonable basis to suspect  
14 or conclude that—

15 “(A) an incident or breach has occurred  
16 with respect to Federal information collected,  
17 used, or maintained by the contractor or award-  
18 ee in connection with the contract, grant, coop-  
19 erative agreement, or other transaction agree-  
20 ment of the contractor or awardee;

21 “(B) an incident or breach has occurred  
22 with respect to a Federal information system  
23 used or operated by the contractor or awardee  
24 in connection with the contract, grant, coopera-

1           tive agreement, or other transaction agreement  
2           of the contractor or awardee;

3           “(C) a component of any Federal informa-  
4           tion system, or a system able to access, store,  
5           or process Federal information, contains a secu-  
6           rity vulnerability, including a supply chain com-  
7           promise or an identified software or hardware  
8           vulnerability; or

9           “(D) the contractor or awardee has re-  
10          ceived information from the agency that the  
11          contractor or awardee is not authorized to re-  
12          ceive in connection with the contract, grant, co-  
13          operative agreement, or other transaction agree-  
14          ment of the contractor or awardee.

15          “(2) PROCEDURES.—

16          “(A) MAJOR INCIDENT.—Following a re-  
17          port of a breach or major incident by a con-  
18          tractor or awardee under paragraph (1), the  
19          agency, in consultation with the contractor or  
20          awardee, shall carry out the requirements under  
21          sections 3592, 3593, and 3594 with respect to  
22          the major incident.

23          “(B) INCIDENT.—Following a report of an  
24          incident by a contractor or awardee under para-  
25          graph (1), an agency, in consultation with the

1 contractor or awardee, shall carry out the re-  
2 quirements under section 3594 with respect to  
3 the incident.

4 “(b) EFFECTIVE DATE.—This section shall apply on  
5 and after the date that is 1 year after the date of the  
6 enactment of the Federal Information Security Mod-  
7 ernization Act of 2022 and shall apply with respect to any  
8 contract entered into on or after such effective date.

9 **“§ 3596. Training**

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

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

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

21 “(2) the obligation of a covered individual to re-  
22 port to the agency a confirmed major incident and  
23 any suspected incident involving information in any  
24 medium or form, including paper, oral, and elec-  
25 tronic.

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

5 **“§ 3597. Analysis and report on Federal incidents**

6       “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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

15                               “(i) attacker tactics, techniques, and  
16 procedures; and

17                               “(ii) system vulnerabilities, including  
18 previously unknown zero day exploitations,  
19 unpatched systems, and information sys-  
20 tem misconfigurations;

21                       “(B) the scope and scale of incidents at  
22 agencies;

23                       “(C) common root causes of incidents  
24 across multiple agencies;

1           “(D) agency incident response, recovery,  
2           and remediation actions and the effectiveness of  
3           those actions, as applicable;

4           “(E) lessons learned and recommendations  
5           in responding to, recovering from, remediating,  
6           and mitigating future incidents; and

7           “(F) trends across multiple Federal agen-  
8           cies to address intrusion detection and incident  
9           response capabilities using the metrics estab-  
10          lished under section 224(c) of the Cybersecurity  
11          Act of 2015 (6 U.S.C. 1522(c)).

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

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

17                 “(A) IN GENERAL.—The Director shall  
18                 share on an ongoing basis the analyses required  
19                 under this subsection with agencies and the Na-  
20                 tional Cyber Director to—

21                         “(i) improve the understanding of cy-  
22                         bersecurity risk of agencies; and

23                         “(ii) support the cybersecurity im-  
24                         provement efforts of agencies.

1           “(B) FORMAT.—In carrying out subpara-  
2 graph (A), the Director shall share the anal-  
3 yses—

4                   “(i) in human-readable written prod-  
5 ucts; and

6                   “(ii) to the greatest extent practicable,  
7 in machine-readable formats in order to  
8 enable automated intake and use by agen-  
9 cies.

10       “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—  
11 Not later than 2 years after the date of the enactment  
12 of this section, and not less frequently than annually  
13 thereafter, the Director of the Cybersecurity and Infra-  
14 structure Security Agency, in consultation with the Direc-  
15 tor, the National Cyber Director, and the heads of other  
16 agencies as appropriate, shall submit to the appropriate  
17 reporting entities a report that includes—

18                   “(1) a summary of causes of incidents from  
19 across the Federal Government that categorizes  
20 those incidents as incidents or major incidents;

21                   “(2) the quantitative and qualitative analyses of  
22 incidents developed under subsection (a)(1) on an  
23 agency-by-agency basis and comprehensively across  
24 the Federal Government, including—

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



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

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

6           “(A) a description of each major incident;  
7           and

8           “(B) an analysis of the agency’s perform-  
9           ance against the metrics established under sec-  
10          tion 224(c) of the Cybersecurity Act of 2015 (6  
11          U.S.C. 1522(c)).

12          “(c) PUBLICATION.—To the extent that publication  
13          is consistent with national security interests, a version of  
14          each report submitted under subsection (b) shall be made  
15          publicly available on the website of the Cybersecurity and  
16          Infrastructure Security Agency during the year in which  
17          the report is submitted.

18          “(d) INFORMATION PROVIDED BY AGENCIES.—

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

23                 “(2) NATIONAL SECURITY SYSTEM REPORTS.—

24                         “(A) IN GENERAL.—Annually, the head of  
25                         an agency that operates or exercises control of

1 a national security system shall submit a report  
2 that includes the information described in sub-  
3 section (b) with respect to the agency to the ex-  
4 tent that the submission is consistent with  
5 standards and guidelines for national security  
6 systems issued in accordance with law and as  
7 directed by the President to—

8 “(i) the majority and minority leaders  
9 of the Senate;

10 “(ii) the Speaker and minority leader  
11 of the House of Representatives;

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

15 “(iv) the Select Committee on Intel-  
16 ligence of the Senate;

17 “(v) the Committee on Armed Serv-  
18 ices of the Senate;

19 “(vi) the Committee on Appropria-  
20 tions of the Senate;

21 “(vii) the Committee on Oversight and  
22 Reform of the House of Representatives;

23 “(viii) the Committee on Homeland  
24 Security of the House of Representatives;

1                   “(ix) the Permanent Select Committee  
2                   on Intelligence of the House of Represent-  
3                   atives;

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

6                   “(xi) the Committee on Appropria-  
7                   tions of the House of Representatives.

8                   “(B) CLASSIFIED FORM.—A report re-  
9                   quired under subparagraph (A) may be sub-  
10                  mitted in a classified form.

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

20               **“§ 3598. Major incident definition**

21               “(a) IN GENERAL.—Not later than 180 days after  
22               the date of the enactment of the Federal Information Se-  
23               curity Modernization Act of 2022, the Director, in coordi-  
24               nation with the Director of the Cybersecurity and Infra-  
25               structure Security Agency and the National Cyber Direc-

1 tor, shall develop and promulgate guidance on the defini-  
2 tion of the term ‘major incident’ for the purposes of sub-  
3 chapter II and this subchapter.

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

7 “(1) include, with respect to any information  
8 collected or maintained by or on behalf of an agency  
9 or an information system used or operated by an  
10 agency or by a contractor of an agency or another  
11 organization on behalf of an agency, any incident  
12 the head of the agency determines is likely to result  
13 in demonstrable harm to—

14 “(A) the national security interests, foreign  
15 relations, or the economy of the United States;

16 “(B) the public confidence, civil liberties,  
17 or public health and safety of the people of the  
18 United States;

19 “(C) the integrity of personally identifiable  
20 information, including the exfiltration, modifica-  
21 tion, or deletion of such information; or

22 “(D) any other type of incident determined  
23 appropriate by the Director; and

24 “(2) stipulate that the Director, in coordination  
25 with the National Cyber Director, shall declare a

1 major incident at each agency impacted by an inci-  
2 dent if it is determined that an incident—

3 “(A) occurs at not less than 2 agencies;

4 “(B) is enabled by—

5 “(i) a common technical root cause,  
6 such as a supply chain compromise or a  
7 common software or hardware vulner-  
8 ability; or

9 “(ii) the related activities of a com-  
10 mon threat actor; or

11 “(C) has a significant impact on the con-  
12 fidentiality, integrity, or availability of a high  
13 value asset.

14 “(c) EVALUATION AND UPDATES.—Not later than 2  
15 years after the date of the enactment of the Federal Infor-  
16 mation Security Modernization Act of 2022, and not less  
17 frequently than every 2 years thereafter, the Director shall  
18 submit to the Committee on Homeland Security and Gov-  
19 ernmental Affairs of the Senate and the Committee on  
20 Oversight and Reform of the House of Representatives an  
21 evaluation, which shall include—

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

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

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

6           (2) CLERICAL AMENDMENT.—The table of sec-  
7 tions for chapter 35 of title 44, United States Code,  
8 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.”.

9 **SEC. 102. AMENDMENTS TO SUBTITLE III OF TITLE 40.**

10           (a) MODERNIZING GOVERNMENT TECHNOLOGY.—  
11 Subtitle G of title X of Division A of the National Defense  
12 Authorization Act for Fiscal Year 2018 (Public Law 115–  
13 91; 40 U.S.C. 11301 note) is amended in section 1078—

14           (1) by striking subsection (a) and inserting the  
15 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.

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

4           (2) in subsection (c)—

5           (A) in paragraph (2)(A)(i), by inserting “,  
6 including a consideration of the impact on high  
7 value assets” after “operational risks”;

8           (B) in paragraph (5)—

9           (i) in subparagraph (A), by striking  
10 “and” at the end;

11           (ii) in subparagraph (B), by striking  
12 the period at the end and inserting “and”;

13           and

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

16           “(C) a senior official from the Cybersecu-  
17 rity and Infrastructure Security Agency of the  
18 Department of Homeland Security, appointed  
19 by the Director.”; and

20           (C) in paragraph (6)(A), by striking “shall  
21 be—” and all that follows through “4 employ-  
22 ees” and inserting “shall be 4 employees”.

23           (b) SUBCHAPTER I.—Subchapter I of chapter 113 of  
24 subtitle III of title 40, United States Code, is amended—

25           (1) in section 11302—

1 (A) in subsection (b), by striking “use, se-  
2 curity, and disposal of” and inserting “use, and  
3 disposal of, and, in consultation with the Direc-  
4 tor of the Cybersecurity and Infrastructure Se-  
5 curity Agency and the National Cyber Director,  
6 promote and improve the security of,”;

7 (B) in subsection (e)(3)(B), by adding at  
8 the end the following:

9 “(iii) The Director may make avail-  
10 able, upon request, to the National Cyber  
11 Director any cybersecurity funding infor-  
12 mation provided to the Director under  
13 clause (ii) of this subparagraph.”;

14 (C) in subsection (f), by striking “The Di-  
15 rector shall” and inserting “The Director  
16 shall—

17 “(1) encourage the heads of the executive agen-  
18 cies to develop and use the best practices in the ac-  
19 quisition of information technology, including supply  
20 chain risk management standards, guidelines, and  
21 practices developed by the National Institute of  
22 Standards and Technology; and

23 “(2) consult with the Federal Chief Information  
24 Security Officer appointed by the President under  
25 section 3607 of title 44, for the development and use



1 of risk management standards, guidelines, and prac-  
2 tices developed by the National Institute of Stand-  
3 ards and Technology.”; and

4 (D) in subsection (h), by inserting “, in-  
5 cluding cybersecurity performances,” after “the  
6 performances”; and

7 (2) in section 11303(b), in paragraph (2)(B)—

8 (A) in clause (i), by striking “or” at the  
9 end;

10 (B) in clause (ii), by adding “or” at the  
11 end; and

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

13 “(iii) whether the function should be  
14 performed by a shared service offered by  
15 another executive agency.”.

16 (c) SUBCHAPTER II.—Subchapter II of chapter 113  
17 of subtitle III of title 40, United States Code, is amend-  
18 ed—

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

21 (2) in section 11313(1), by striking “efficiency  
22 and effectiveness” and inserting “efficiency, security,  
23 and effectiveness”;

24 (3) in section 11315, by adding at the end the  
25 following:

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

4 “(1) the Chief Information Officer designated  
5 under section 3506(a)(2) of title 44 or an equivalent  
6 official of the agency of which the component agency  
7 is a component; and

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

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

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

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

16 (1) in subsection (a), by striking “section  
17 3532(b)(1)” and inserting “section 3552(b)”;

18 (2) in subsection (b)(1)(A), by striking “the  
19 Secretary of Homeland Security” and inserting “the  
20 Director of the Cybersecurity and Infrastructure Se-  
21 curity Agency”; and

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

23 “(e) REVIEW OF OFFICE OF MANAGEMENT AND  
24 BUDGET GUIDANCE AND POLICY.—

25 “(1) CONDUCT OF REVIEW.—

1           “(A) IN GENERAL.—Not less frequently  
2 than once every 3 years, the Director of the Of-  
3 fice of Management and Budget, in consultation  
4 with, as available, the Chief Information Offi-  
5 cers Council, the Director of the Cybersecurity  
6 and Infrastructure Security Agency, the Na-  
7 tional Cyber Director, the Comptroller General  
8 of the United States, and the Council of the In-  
9 spectors General on Integrity and Efficiency,  
10 shall review the efficacy of the guidance and  
11 policy promulgated by the Director in reducing  
12 cybersecurity risks, including an assessment of  
13 the requirements for agencies to report infor-  
14 mation to the Director, and determine whether  
15 any changes to that guidance or policy is appro-  
16 priate.

17           “(B) FEDERAL RISK ASSESSMENTS.—In  
18 conducting the review described in subpara-  
19 graph (A), the Director shall consider the Fed-  
20 eral risk assessments performed under section  
21 3553(i) of title 44.

22           “(C) REQUIREMENTS BURDEN REDUCTION  
23 AND CLARITY.—In conducting the review de-  
24 scribed in subparagraph (A), the Director shall  
25 consider the cumulative reporting and compli-

1           ance burden to agencies as well as the clarity  
2           of the requirements and deadlines contained in  
3           guidance and policy documents.

4           “(2) UPDATED GUIDANCE.—Not later than 90  
5           days after the date on which a review is completed  
6           under paragraph (1), the Director of the Office of  
7           Management and Budget shall issue updated guid-  
8           ance or policy to agencies determined appropriate by  
9           the Director, based on the results of the review.

10          “(3) CONGRESSIONAL BRIEFING.—Not later  
11          than 60 days after the date on which a review is  
12          completed under paragraph (1), the Director is ex-  
13          pected to provide to the Committee on Homeland  
14          Security and Governmental Affairs of the Senate  
15          and the Committee on Oversight and Reform of the  
16          House of Representatives a briefing on the review  
17          and any newly issued guidance or policy, which shall  
18          include—

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

22                 “(B) the cybersecurity risk mitigation, or  
23                 other cybersecurity benefit, offered by each  
24                 guidance or policy document described in sub-  
25                 paragraph (A); and

1           “(C) a summary of the guidance or policy  
2           to which changes were determined appropriate  
3           during the review and what the changes in-  
4           clude.

5           “(f) AUTOMATED STANDARD IMPLEMENTATION  
6 VERIFICATION.—When the Director of the National Insti-  
7 tute of Standards and Technology issues a proposed  
8 standard pursuant to paragraphs (2) and (3) of section  
9 20(a) of the National Institute of Standards and Tech-  
10 nology Act (15 U.S.C. 278g–3(a)), the Director of the Na-  
11 tional Institute of Standards and Technology shall con-  
12 sider developing and, if appropriate and practical, develop,  
13 in consultation with the Director of the Cybersecurity and  
14 Infrastructure Security Agency, specifications to enable  
15 the automated verification of the implementation of con-  
16 trols.”.

17 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**  
18 **SPONSE.**

19           (a) RESPONSIBILITIES OF THE CYBERSECURITY AND  
20 INFRASTRUCTURE SECURITY AGENCY.—

21           (1) IN GENERAL.—Not later than 180 days  
22           after the date of the enactment of this Act, the Di-  
23           rector of the Cybersecurity and Infrastructure Secu-  
24           rity Agency shall—

1 (A) develop a plan for the development of  
2 the analysis required under section 3597(a) of  
3 title 44, United States Code, as added by this  
4 Act, and the report required under subsection  
5 (b) of that section that includes—

6 (i) a description of any challenges the  
7 Director anticipates encountering; and

8 (ii) the use of automation and ma-  
9 chine-readable formats for collecting, com-  
10 piling, monitoring, and analyzing data; and

11 (B) provide to the appropriate congres-  
12 sional committees a briefing on the plan devel-  
13 oped under subparagraph (A).

14 (2) BRIEFING.—Not later than 1 year after the  
15 date of the enactment of this Act, the Director of  
16 the Cybersecurity and Infrastructure Security Agen-  
17 cy shall provide to the appropriate congressional  
18 committees a briefing on—

19 (A) the execution of the plan required  
20 under paragraph (1)(A); and

21 (B) the development of the report required  
22 under section 3597(b) of title 44, United States  
23 Code, as added by this Act.

24 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE  
25 OFFICE OF MANAGEMENT AND BUDGET.—

1           (1) FISMA.—Section 2 of the Federal Informa-  
2           tion Security Modernization Act of 2014 (Public  
3           Law 113–283; 44 U.S.C. 3554 note) is amended—

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

5                   (B) by redesignating subsections (c)  
6           through (f) as subsections (b) through (e), re-  
7           spectively.

8           (2) IN GENERAL.—The Director shall develop  
9           guidance, to be updated not less frequently than  
10          once every 2 years, on the content, timeliness, and  
11          format of the information provided by agencies  
12          under section 3594(a) of title 44, United States  
13          Code, as added by this Act.

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

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

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

6 (5) CONTRACTOR AND AWARDEE GUIDANCE.—

7 (A) IN GENERAL.—Not later than 1 year  
8 after the date of the enactment of this Act, the  
9 Director, 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 Act.

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  
18 of the requesting agency has made a written request  
19 to the agency that maintains the record specifying  
20 the particular portion desired and the activity for  
21 which the record is sought.”.

1 **SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**  
2 **UPDATES.**

3 Not later than 1 year after the date of the enactment  
4 of this Act, the Director shall issue guidance for agencies  
5 on—

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

10 (2) implementing additional cybersecurity pro-  
11 cedures, which shall include resources for shared  
12 services;

13 (3) establishing a process for providing the sta-  
14 tus of each remedial action under section 3554(b)(7)  
15 of title 44, United States Code, as amended by this  
16 Act, to the Director and the Director of the Cyberse-  
17 curity and Infrastructure Security Agency using au-  
18 tomation and machine-readable data, as practicable,  
19 which shall include—

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

22 (B) templates for providing the status of  
23 the remedial action;

24 (4) interpreting the definition of “high value  
25 asset” under section 3552 of title 44, United States  
26 Code, as amended by this Act; and

1           (5) a requirement to coordinate with inspectors  
2           general of agencies to ensure consistent under-  
3           standing and application of agency policies for the  
4           purpose of evaluations by inspectors general.

5 **SEC. 105. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**  
6                           **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

7           (a) DEFINITIONS.—In this section:

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

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

15                  (b).

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

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

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

## 4   **TITLE II—IMPROVING FEDERAL** 5                           **CYBERSECURITY**

### 6   **SEC. 201. MOBILE SECURITY STANDARDS.**

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

9                   (1) evaluate mobile application security guid-  
10           ance promulgated by the Director; and

11                   (2) issue guidance to secure mobile devices, in-  
12           cluding for mobile applications, for every agency.

13           (b) CONTENTS.—The guidance issued under sub-  
14           section (a)(2) shall include—

15                   (1) a requirement, pursuant to section  
16           3506(b)(4) of title 44, United States Code, for every  
17           agency to maintain a continuous inventory of  
18           every—

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

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

23                   (2) a requirement for every agency to perform  
24           continuous evaluation of the vulnerabilities described

1 in paragraph (1)(B) and other risks associated with  
2 the use of applications on mobile devices.

3 (c) INFORMATION SHARING.—The Director, in co-  
4 ordination with the Director of the Cybersecurity and In-  
5 frastructure Security Agency, shall issue guidance to  
6 agencies for sharing the inventory of the agency required  
7 under subsection (b)(1) with the Director of the Cyberse-  
8 curity and Infrastructure Security Agency, using automa-  
9 tion and machine-readable data to the greatest extent  
10 practicable.

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

17 **SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT**  
18 **RESPONSE.**

19 (a) RECOMMENDATIONS.—Not later than 2 years  
20 after the date of the enactment of this Act, and not less  
21 frequently than every 2 years thereafter, the Director of  
22 the Cybersecurity and Infrastructure Security Agency, in  
23 consultation with the Attorney General, shall submit to  
24 the Director recommendations on requirements for logging

1 events on agency systems and retaining other relevant  
2 data within the systems and networks of an agency.

3 (b) CONTENTS.—The recommendations provided  
4 under subsection (a) shall include—

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

6 (2) the duration that logs and other relevant  
7 data should be retained;

8 (3) the time periods for agency implementation  
9 of recommended logging and security requirements;

10 (4) how to ensure the confidentiality, integrity,  
11 and availability of logs;

12 (5) requirements to ensure that, upon request,  
13 in a manner that excludes or otherwise reasonably  
14 protects personally identifiable information, and to  
15 the extent permitted by applicable law (including  
16 privacy and statistical laws), agencies provide logs  
17 to—

18 (A) the Director of the Cybersecurity and  
19 Infrastructure Security Agency for a cybersecu-  
20 rity purpose; and

21 (B) the Director of the Federal Bureau of  
22 Investigation, or the appropriate Federal law  
23 enforcement agency, to investigate potential  
24 criminal activity; and

1           (6) requirements to ensure that, subject to com-  
2           pliance with statistical laws and other relevant data  
3           protection requirements, the highest level security  
4           operations center of each agency has visibility into  
5           all agency logs.

6           (c) GUIDANCE.—Not later than 90 days after receiv-  
7           ing the recommendations submitted under subsection (a),  
8           the Director, in consultation with the Director of the Cy-  
9           bersecurity and Infrastructure Security Agency and the  
10          Attorney General, shall, as determined to be appropriate  
11          by the Director, update guidance to agencies regarding re-  
12          quirements for logging, log retention, log management,  
13          sharing of log data with other appropriate agencies, or any  
14          other logging activity determined to be appropriate by the  
15          Director.

16          (d) SUNSET.—This section will cease to be in effect  
17          on the date that is 10 years after the date of the enact-  
18          ment of this Act.

19          **SEC. 203. FEDERAL PENETRATION TESTING POLICY.**

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

23          **“§ 3559A. Federal penetration testing**

24          “(a) GUIDANCE.—

1           “(1) IN GENERAL.—The Director shall, in con-  
2           sultation with the Secretary of the Department of  
3           Homeland Security acting through the Director of  
4           the Cybersecurity and Infrastructure Security Agen-  
5           cy, issue guidance to agencies that—

6                   “(A) requires agencies to use, when and  
7                   where appropriate, penetration testing on agen-  
8                   cy systems by both Federal and non-Federal en-  
9                   tities, with a focus on high value assets;

10                   “(B) provides policies governing agency de-  
11                   velopment of an operational plan, rules of en-  
12                   gagement for utilizing penetration testing, and  
13                   procedures to utilize the results of penetration  
14                   testing to improve the cybersecurity and risk  
15                   management of the agency; and

16                   “(C) establishes a program under the Cy-  
17                   bersecurity and Infrastructure Security Agency  
18                   to ensure that penetration testing is being per-  
19                   formed appropriately by agencies and to provide  
20                   operational support or a shared service.

21           “(b) RESPONSIBILITIES OF OMB.—The Director, in  
22           coordination with the Director of the Cybersecurity and  
23           Infrastructure Security Agency, shall—

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



1           “(2) develop and maintain a standardized pro-  
2           cess for the use of penetration testing.

3           “(c) EXCEPTION FOR NATIONAL SECURITY SYS-  
4           TEMS.—The guidance issued under subsection (a) shall  
5           not apply to national security systems.

6           “(d) DELEGATION OF AUTHORITY FOR CERTAIN  
7           SYSTEMS.—The authorities of the Director described in  
8           subsection (a) shall be delegated—

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

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

13           (b) DEADLINE FOR GUIDANCE.—Not later than 180  
14           days after the date of the enactment of this Act, the Direc-  
15           tor shall issue the guidance required under section  
16           3559A(a) of title 44, United States Code, as added by sub-  
17           section (a).

18           (c) SUNSET.—This section shall sunset on the date  
19           that is 10 years after the date of the enactment of this  
20           Act.

21           (d) CLERICAL AMENDMENT.—The table of sections  
22           for chapter 35 of title 44, United States Code, is amended  
23           by adding after the item relating to section 3559 the fol-  
24           lowing:

“3559A. Federal penetration testing.”.

1 (e) PENETRATION TESTING BY THE SECRETARY OF  
2 HOMELAND SECURITY.—Section 3553(b) of title 44,  
3 United States Code, as amended by section 5121, is fur-  
4 ther amended—

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

7 (2) by redesignating paragraph (9) as para-  
8 graph (10); and

9 (3) by inserting after paragraph (8) the fol-  
10 lowing:

11 “(9) performing penetration testing to identify  
12 vulnerabilities within Federal information systems;  
13 and”.

14 **SEC. 204. ONGOING THREAT HUNTING PROGRAM.**

15 (a) THREAT HUNTING PROGRAM.—

16 (1) IN GENERAL.—Not later than 540 days  
17 after the date of the enactment of this Act, the Di-  
18 rector of the Cybersecurity and Infrastructure Secu-  
19 rity Agency shall, in accordance with the authorities  
20 granted the Secretary under sections 3553(b)(7)–(8)  
21 and 3553(m) of title 44, United States Code (as re-  
22 designated by this Act), establish a program to pro-  
23 vide ongoing, hypothesis-driven threat-hunting serv-  
24 ices on the network of each agency.

1           (2) PLAN.—Not later than 180 days after the  
2 date of the enactment of this Act, the Director of  
3 the Cybersecurity and Infrastructure Security Agen-  
4 cy shall develop a plan to establish the program re-  
5 quired under paragraph (1) that describes how the  
6 Director of the Cybersecurity and Infrastructure Se-  
7 curity Agency plans to—

8           (A) determine the method for collecting,  
9 storing, accessing, analyzing, and safeguarding  
10 appropriate agency data;

11           (B) provide on-premises support to agen-  
12 cies;

13           (C) staff threat hunting services;

14           (D) allocate available human and financial  
15 resources to implement the plan; and

16           (E) provide input to the heads of agencies  
17 on the use of—

18           (i) more stringent standards under  
19 section 11331(c)(1) of title 40, United  
20 States Code; and

21           (ii) additional cybersecurity proce-  
22 dures under section 3554 of title 44,  
23 United States Code.

24           (b) REPORTS.—The Director of the Cybersecurity  
25 and Infrastructure Security Agency, in consultation with

1 the Director, shall submit to the appropriate congressional  
2 committees—

3 (1) not later than 30 days after the date on  
4 which the Director of the Cybersecurity and Infra-  
5 structure Security Agency completes the plan re-  
6 quired under subsection (a)(2), a report on the plan  
7 to provide threat hunting services to agencies;

8 (2) not less than 30 days before the date on  
9 which the Director of the Cybersecurity and Infra-  
10 structure Security Agency begins providing threat  
11 hunting services under the program under sub-  
12 section (a)(1), a report providing any updates to the  
13 plan developed under subsection (a)(2); and

14 (3) not later than 1 year after the date on  
15 which the Director of the Cybersecurity and Infra-  
16 structure Security Agency begins providing threat  
17 hunting services to agencies other than the Cyberse-  
18 curity and Infrastructure Security Agency, a report  
19 describing lessons learned from providing those serv-  
20 ices.

21 **SEC. 205. CODIFYING VULNERABILITY DISCLOSURE PRO-**  
22 **GRAMS.**

23 (a) IN GENERAL.—Subchapter II of Chapter 35 of  
24 title 44, United States Code, is amended by inserting after  
25 section 3559A, as added by section 204, the following:

1 **“§ 3559B. Federal vulnerability disclosure programs**

2 “(a) DEFINITIONS.—In this section:

3 “(1) REPORT.—The term ‘report’ means a vul-  
4 nerability disclosure made to an agency by a re-  
5 porter.

6 “(2) REPORTER.—The term ‘reporter’ means  
7 an individual that submits a vulnerability report  
8 pursuant to the vulnerability disclosure process of an  
9 agency.

10 “(b) RESPONSIBILITIES OF OMB.—

11 “(1) LIMITATION ON LEGAL ACTION.—The Di-  
12 rector of the Office of Management and Budget, in  
13 consultation with the Attorney General, shall issue  
14 guidance to agencies to not recommend or pursue  
15 legal action against a reporter or an individual that  
16 conducts a security research activity that the head  
17 of the agency determines—

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

21 “(B) is authorized under the vulnerability  
22 disclosure policy of the agency developed under  
23 subsection (d)(2).

24 “(2) SHARING INFORMATION WITH CISA.—The  
25 Director of the Office of Management and Budget,  
26 in coordination with the Director of the Cybersecu-

1 rity and Infrastructure Security Agency and in con-  
2 sultation with the National Cyber Director, shall  
3 issue guidance to agencies on sharing relevant infor-  
4 mation in a consistent, automated, and machine  
5 readable manner with the Director of the Cybersecu-  
6 rity and Infrastructure Security Agency, including—

7 “(A) any valid or credible reports of newly  
8 discovered or not publicly known vulnerabilities  
9 (including misconfigurations) on Federal infor-  
10 mation systems that use commercial software or  
11 services;

12 “(B) information relating to vulnerability  
13 disclosure, coordination, or remediation activi-  
14 ties of an agency, particularly as those activities  
15 relate to outside organizations—

16 “(i) with which the head of the agency  
17 believes the Director of the Cybersecurity  
18 and Infrastructure Security Agency can as-  
19 sist; or

20 “(ii) about which the head of the  
21 agency believes the Director of the Cyber-  
22 security and Infrastructure Security Agen-  
23 cy should know; and

24 “(C) any other information with respect to  
25 which the head of the agency determines helpful

1 or necessary to involve the Director of the Cy-  
2 bersecurity and Infrastructure Security Agency.

3 “(3) AGENCY VULNERABILITY DISCLOSURE  
4 POLICIES.—The Director shall issue guidance to  
5 agencies on the required minimum scope of agency  
6 systems covered by the vulnerability disclosure policy  
7 of an agency required under subsection (d)(2).

8 “(c) RESPONSIBILITIES OF CISA.—The Director of  
9 the Cybersecurity and Infrastructure Security Agency  
10 shall—

11 “(1) provide support to agencies with respect to  
12 the implementation of the requirements of this sec-  
13 tion;

14 “(2) develop tools, processes, and other mecha-  
15 nisms determined appropriate to offer agencies capa-  
16 bilities to implement the requirements of this sec-  
17 tion; and

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

21 “(d) RESPONSIBILITIES OF AGENCIES.—

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

1           “(A) an appropriate security contact; and

2           “(B) the component of the agency that is  
3 responsible for the internet accessible services  
4 offered at the domain.

5           “(2) VULNERABILITY DISCLOSURE POLICY.—

6 The head of each agency shall develop and make  
7 publicly available a vulnerability disclosure policy for  
8 the agency, which shall—

9           “(A) describe—

10           “(i) the scope of the systems of the  
11 agency included in the vulnerability disclo-  
12 sure policy;

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

15           “(iii) the type of information system  
16 testing that is not authorized by the agen-  
17 cy; and

18           “(iv) the disclosure policy of the agen-  
19 cy for sensitive information;

20           “(B) with respect to a report to an agency,  
21 describe—

22           “(i) how the reporter should submit  
23 the report; and

24           “(ii) if the report is not anonymous,  
25 when the reporter should anticipate an ac-



1 knowledge of receipt of the report by  
2 the agency;

3 “(C) include any other relevant informa-  
4 tion; and

5 “(D) be mature in scope, covering all inter-  
6 net accessible Federal information systems used  
7 or operated by that agency or on behalf of that  
8 agency.

9 “(3) IDENTIFIED VULNERABILITIES.—The head  
10 of each agency shall incorporate any vulnerabilities  
11 reported under paragraph (2) into the vulnerability  
12 management process of the agency in order to track  
13 and remediate the vulnerability.

14 “(e) CONGRESSIONAL REPORTING.—Not later than  
15 90 days after the date of the enactment of the Federal  
16 Information Security Modernization Act of 2022, and an-  
17 nually thereafter for a 3-year period, the Director of the  
18 Cybersecurity and Infrastructure Security Agency, in con-  
19 sultation with the Director, shall provide to the Committee  
20 on Homeland Security and Governmental Affairs of the  
21 Senate and the Committee on Oversight and Reform of  
22 the House of Representatives a briefing on the status of  
23 the use of vulnerability disclosure policies under this sec-  
24 tion at agencies, including, with respect to the guidance

1 issued under subsection (b)(3), an identification of the  
2 agencies that are compliant and not compliant.

3 “(f) EXEMPTIONS.—The authorities and functions of  
4 the Director and Director of the Cybersecurity and Infra-  
5 structure Security Agency under this section shall not  
6 apply to national security systems.

7 “(g) DELEGATION OF AUTHORITY FOR CERTAIN  
8 SYSTEMS.—The authorities of the Director and the Direc-  
9 tor of the Cybersecurity and Infrastructure Security Agen-  
10 cy described in this section shall be delegated—

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

13 “(2) to the Director of National Intelligence in  
14 the case of systems described in section  
15 3553(e)(3).”.

16 (b) SUNSET.—This section shall sunset on the date  
17 that is 10 years after the date of the enactment of this  
18 Act.

19 (c) CLERICAL AMENDMENT.—The table of sections  
20 for chapter 35 of title 44, United States Code, is amended  
21 by adding after the item relating to section 3559A, as  
22 added by this Act, the following:

“3559B. Federal vulnerability disclosure programs.”.

23 **SEC. 206. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

24 (a) GUIDANCE.—The Director shall maintain guid-  
25 ance on the adoption of zero trust architecture and not

1 later than 2 years after the date of the enactment of this  
2 Act, provide an update to the appropriate congressional  
3 committees on progress in increasing the internal defenses  
4 of agency systems through such adoption across the gov-  
5 ernment, including—

6 (1) shifting away from “trusted networks” to  
7 implement security controls based on a presumption  
8 of compromise;

9 (2) implementing principles of least privilege in  
10 administering information security programs;

11 (3) limiting the ability of entities that cause in-  
12 cidents to move laterally through or between agency  
13 systems;

14 (4) identifying incidents quickly;

15 (5) isolating and removing unauthorized entities  
16 from agency systems as quickly as practicable, ac-  
17 counting for intelligence or law enforcement pur-  
18 poses;

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

21 (7) a summary of the agency progress reports  
22 required under subsection (b).

23 (b) AGENCY PROGRESS REPORTS.—Not later than  
24 270 days after the date of the enactment of this Act, the  
25 head of each agency shall submit to the Director a

1 progress report on implementing an information security  
2 program based on a zero trust architecture, which shall  
3 include—

4 (1) a description of any steps the agency has  
5 completed, including progress toward achieving any  
6 requirements issued by the Director, including the  
7 adoption of any models or reference architecture;

8 (2) an identification of activities that have not  
9 yet been completed and that would have the most  
10 immediate security impact; and

11 (3) a schedule to implement any planned activi-  
12 ties.

13 **SEC. 207. GAO AUTOMATION REPORT.**

14 Not later than 2 years after the date of the enact-  
15 ment of this Act, the Comptroller General of the United  
16 States shall perform a study on the use of automation and  
17 machine-readable data across the Federal Government for  
18 cybersecurity purposes, including the automated updating  
19 of cybersecurity tools, sensors, or processes employed by  
20 agencies under paragraphs (1), (5)(C), and (8)(B) of sec-  
21 tion 3554(b) of title 44, United States Code.

1 **SEC. 208. EXTENSION OF FEDERAL ACQUISITION SECURITY**  
2 **COUNCIL.**

3 (a) **EXTENSION.**—Section 1328 of title 41, United  
4 States Code, is amended by striking “the date that” and  
5 all that follows and inserting “December 31, 2026”.

6 (b) **DESIGNATION.**—Section 1322(c)(1) of title 41,  
7 United States Code, is amended by striking “Not later  
8 than” and all that follows through the end of the para-  
9 graph and inserting the following: “The Director of OMB  
10 shall designate the Federal Chief Information Security Of-  
11 ficer appointed by the President under section 3607 of  
12 title 44, or an equivalent senior-level official from the Of-  
13 fice of Management and Budget if the position is vacant,  
14 to serve as the Chairperson of the Council.”.

15 (c) **REQUIREMENT.**—Subsection 1326(b) of title 41,  
16 United States Code, is amended—

17 (1) in paragraph (5), by striking “; and” and  
18 inserting a semicolon;

19 (2) by redesignating paragraph (6) as para-  
20 graph (7); and

21 (3) by inserting after paragraph (5) the fol-  
22 lowing new paragraph:

23 “(6) maintaining an up-to-date and accurate in-  
24 ventory of software in use by the agency and, when  
25 available, the components of such software, including  
26 any available Software Bills of Materials, as applica-

1 ble, that can be communicated when requested to  
 2 the Federal Acquisition Security Council, the Na-  
 3 tional Cybersecurity Director, or the Secretary of  
 4 Homeland Security acting through the Director of  
 5 Cybersecurity and Infrastructure Security Agency.”.

6 **SEC. 209. FEDERAL CHIEF INFORMATION SECURITY OFFI-**  
 7 **CER.**

8 (a) AMENDMENT.—Chapter 36 of title 44, United  
 9 States Code, is amended by inserting at the end:

10 **“§ 3607. Federal chief information security officer**

11 “(a) ESTABLISHMENT.—There is established in the  
 12 Office of the Federal Chief Information Officer of the Of-  
 13 fice of Management and Budget a Federal Chief Informa-  
 14 tion Security Officer, who shall be appointed by the Presi-  
 15 dent.

16 “(b) DUTIES.—The Federal Chief Information Secu-  
 17 rity Officer shall report to the Federal Chief Information  
 18 Officer, and assist the Chief Information Officer in car-  
 19 rying out—

20 “(1) all functions under this chapter;

21 “(2) all functions assigned to the Director  
 22 under title II of the E–Government Act of 2002;

23 “(3) other electronic government initiatives,  
 24 consistent with other statutes;

1           “(4) assisting the Director with carrying out  
2 budget formation duties under subtitle II of title 31  
3 as it pertains to the information technology, oper-  
4 ations, and workforce resources of Federal agencies  
5 to fulfill cybersecurity responsibilities under section  
6 3554, and the duties of the Department of Home-  
7 land Security duties designated under section 3553;  
8 and

9           “(5) other initiatives determined by the Chief  
10 Information Officer.

11       “(c) ADDITIONAL DUTIES.—The Federal Chief Infor-  
12 mation Security Officer shall work with the Chief Informa-  
13 tion Officer to oversee implementation of electronic Gov-  
14 ernment under the E–Government Act of 2002, and other  
15 relevant statutes, in a manner consistent with law, relating  
16 to—

17           “(1) cybersecurity strategy, policy, and oper-  
18 ations, including the performance of the duties of  
19 the Director under subchapter II of chapter 35;

20           “(2) the development of enterprise architec-  
21 tures;

22           “(3) information security;

23           “(4) privacy;

24           “(5) access to, dissemination of, and preserva-  
25 tion of Government information; and

1           “(6) other areas of electronic Government as  
2           determined by the Administrator.

3           “(d) ASSISTANCE.—The Federal Chief Information  
4 Security Officer shall assist the Administrator in the per-  
5 formance of electronic Government functions as described  
6 in section 3602(f).”.

7           (b) DEPUTY NATIONAL CYBER DIRECTOR.—Section  
8 1752 of the William M. (Mac) Thornberry National De-  
9 fense Authorization Act for Fiscal Year 2021 (6 U.S.C.  
10 1500; 134 Stat. 4144) is amended by adding at the end  
11 the following new subsection:

12           “(d) DEPUTY DIRECTOR.—There shall be a Deputy  
13 National Cyber Director for Agency Strategy, Capabilities,  
14 and Budget, who shall be the Federal Chief Information  
15 Security Officer appointed by the President under section  
16 3607 of title 44, United States Code, and shall report to  
17 the Director and assist the office in carrying out the fol-  
18 lowing duties as it applies to the protection of Federal in-  
19 formation systems by the agencies—

20           “(1) the preparation and oversight over the im-  
21 plementation of national cyber policy and strategy  
22 under subsection (c)(1)(C)(i);

23           “(2) the formation and issuance of rec-  
24 ommendations to agencies on resource allocations  
25 and policies under subsection (c)(1)(C)(ii);





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

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

5                   “(B) that shall include a dashboard of  
6           open information security recommendations  
7           identified in the independent evaluations re-  
8           quired by section 3555(a) of title 44, United  
9           States Code; and”.

10 **SEC. 212. QUANTITATIVE CYBERSECURITY METRICS.**

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

15           (b) UPDATING AND ESTABLISHING METRICS.—Not  
16           later than 1 year after the date of the enactment of this  
17           Act, the Director of the Cybersecurity and Infrastructure  
18           Security Agency, in coordination with the Director and  
19           consulting with the Director of the National Institute of  
20           Standards and Technology, shall—

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

23                   (2) as appropriate and pursuant to section  
24           224(c) of the Cybersecurity Act of 2015 (6 U.S.C.  
25           1522(c))—

1 (A) update the covered metrics; and

2 (B) establish new covered metrics.

3 (c) IMPLEMENTATION.—

4 (1) IN GENERAL.—Not later than 540 days  
5 after the date of the enactment of this Act, the Di-  
6 rector, in coordination with the Director of the Cy-  
7 bersecurity and Infrastructure Security Agency,  
8 shall promulgate guidance that requires each agency  
9 to use covered metrics to track trends in the cyber-  
10 security and incident response capabilities of the  
11 agency.

12 (2) PERFORMANCE DEMONSTRATION.—The  
13 guidance issued under paragraph (1) and any subse-  
14 quent guidance shall require agencies to share with  
15 the Director of the Cybersecurity and Infrastructure  
16 Security Agency data demonstrating the perform-  
17 ance of the agency using the covered metrics in-  
18 cluded in the guidance.

19 (3) PENETRATION TESTS.—On not less than 2  
20 occasions during the 2-year period following the date  
21 on which guidance is promulgated under paragraph  
22 (1), the Director shall ensure that not less than 3  
23 agencies are subjected to substantially similar pene-  
24 tration tests, as determined by the Director, in co-  
25 ordination with the Director of the Cybersecurity

1 and Infrastructure Security Agency, in order to vali-  
2 date the utility of the covered metrics.

3 (4) ANALYSIS CAPACITY.—The Director of the  
4 Cybersecurity and Infrastructure Security Agency  
5 shall develop a capability that allows for the analysis  
6 of the covered metrics, including cross-agency per-  
7 formance of agency cybersecurity and incident re-  
8 sponse capability trends.

9 (d) CONGRESSIONAL REPORTS.—

10 (1) UTILITY OF METRICS.—Not later than 1  
11 year after the date of the enactment of this Act, the  
12 Director of the Cybersecurity and Infrastructure Se-  
13 curity Agency, in coordination with the Director,  
14 shall submit to the appropriate congressional com-  
15 mittees a report on the utility of the covered metrics.

16 (2) USE OF METRICS.—Not later than 180 days  
17 after the date on which the Director promulgates  
18 guidance under subsection (c)(1), the Director shall  
19 submit to the appropriate congressional committees  
20 a report on the results of the use of the covered  
21 metrics by agencies.

22 (e) FEDERAL CYBERSECURITY ENHANCEMENT ACT  
23 OF 2015 UPDATES.—The Federal Cybersecurity Enhance-  
24 ment Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

1 (1) in section 222(3)(B), by inserting “and the  
2 Committee on Oversight and Reform” before “of the  
3 House of Representatives”; and

4 (2) in section 224—

5 (A) by amending subsection (c) to read as  
6 follows:

7 “(c) IMPROVED METRICS.—The Director of the Cy-  
8 bersecurity and Infrastructure Security Agency, in coordi-  
9 nation with the Director, shall establish, review, and up-  
10 date metrics to measure the cybersecurity and incident re-  
11 sponse capabilities of agencies in accordance with the re-  
12 sponsibilities of agencies under section 3554 of title 44,  
13 United States Code.”;

14 (B) by striking subsection (e); and

15 (C) by redesignating subsection (f) as sub-  
16 section (e).

17 **TITLE III—PILOT PROGRAMS TO**  
18 **ENHANCE FEDERAL CYBER-**  
19 **SECURITY**

20 **SEC. 301. RISK-BASED BUDGET PILOT.**

21 (a) DEFINITIONS.—In this section:

22 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
23 TEES.—The term “appropriate congressional com-  
24 mittees” means—

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

4 (B) the Committee on Homeland Security,  
5 the Committee on Oversight and Reform, and  
6 the Committee on Appropriations of the House  
7 of Representatives.

8 (2) INFORMATION TECHNOLOGY.—The term  
9 “information technology”—

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

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

16 (3) RISK-BASED BUDGET.—The term “risk-  
17 based budget” means a budget—

18 (A) developed by identifying and  
19 prioritizing cybersecurity risks and  
20 vulnerabilities, including impact on agency oper-  
21 ations in the case of a cyber attack, through  
22 analysis of cyber threat intelligence, incident  
23 data, and tactics, techniques, procedures, and  
24 capabilities of cyber threats; and

1 (B) that allocates resources based on the  
2 risks identified and prioritized under subpara-  
3 graph (A).

4 (b) ESTABLISHMENT OF RISK-BASED BUDGET  
5 PILOT.—

6 (1) IN GENERAL.—

7 (A) MODEL.—Not later than 1 year after  
8 the first publication of the budget submitted by  
9 the President under section 1105 of title 31,  
10 United States Code, following the date of the  
11 enactment of this Act, the Director, in consulta-  
12 tion with the Director of the Cybersecurity and  
13 Infrastructure Security Agency and the Na-  
14 tional Cyber Director and in coordination with  
15 the Director of the National Institute of Stand-  
16 ards and Technology, shall conduct a pilot for  
17 creating a risk-based budget for cybersecurity  
18 spending.

19 (B) CONTENTS OF PILOT.—The pilot re-  
20 quired to be developed under this paragraph  
21 shall—

22 (i) consider Federal and non-Federal  
23 cyber threat intelligence products, where  
24 available, to identify threats,  
25 vulnerabilities, and risks;

1 (ii) consider the impact on agency op-  
2 erations of incidents, including the  
3 interconnectivity to other agency systems  
4 and the operations of other agencies;

5 (iii) indicate where resources should  
6 be allocated to have the greatest impact on  
7 mitigating current and future threats and  
8 current and future cybersecurity capabili-  
9 ties;

10 (iv) be used to inform acquisition and  
11 sustainment of—

12 (I) information technology and  
13 cybersecurity tools;

14 (II) information technology and  
15 cybersecurity architectures;

16 (III) information technology and  
17 cybersecurity personnel; and

18 (IV) cybersecurity and informa-  
19 tion technology concepts of operations;  
20 and

21 (v) be used to evaluate and inform  
22 government-wide cybersecurity programs of  
23 the Department of Homeland Security.

24 (2) REPORTS.—Not later than 2 years after the  
25 first publication of the budget submitted by the



1 President under section 1105 of title 31, United  
2 States Code, following the date of the enactment of  
3 this Act, the Director shall submit a report to Con-  
4 gress on the implementation of the pilot for risk-  
5 based budgeting for cybersecurity spending, an as-  
6 sessment of agency implementation, and an evalua-  
7 tion of whether the risk-based budget helps to miti-  
8 gate cybersecurity vulnerabilities.

9 (3) GAO REPORT.—Not later than 3 years  
10 after the date on which the first budget of the Presi-  
11 dent is submitted to Congress containing the valida-  
12 tion required under section 1105(a)(35)(A)(i)(V) of  
13 title 31, United States Code, as amended by sub-  
14 section (c), the Comptroller General of the United  
15 States shall submit to the appropriate congressional  
16 committees a report that includes—

17 (A) an evaluation of the success of pilot  
18 agencies in implementing risk-based budgets;

19 (B) an evaluation of whether the risk-  
20 based budgets developed by pilot agencies are  
21 effective at informing Federal Government-wide  
22 cybersecurity programs; and

23 (C) any other information relating to risk-  
24 based budgets the Comptroller General deter-  
25 mines appropriate.

1 **SEC. 302. ACTIVE CYBER DEFENSIVE STUDY.**

2 (a) DEFINITION.—In this section, the term “active  
3 defense technique” has the meaning given in guidance  
4 issued by the Director, in coordination with the Attorney  
5 General.

6 (b) STUDY.—Not later than 180 days after the date  
7 of the enactment of this Act, the Director of the Cyberse-  
8 curity and Infrastructure Security Agency, in coordination  
9 with the Director and the National Cyber Director, shall  
10 perform a study on the use of active defense techniques  
11 to enhance the security of agencies, which shall include—

12 (1) a review of legal restrictions on the use of  
13 different active cyber defense techniques in Federal  
14 environments, in consultation with the Attorney  
15 General;

16 (2) an evaluation of—

17 (A) the efficacy of a selection of active de-  
18 fense techniques determined by the Director of  
19 the Cybersecurity and Infrastructure Security  
20 Agency; and

21 (B) factors that impact the efficacy of the  
22 active defense techniques evaluated under sub-  
23 paragraph (A);

24 (3) recommendations on safeguards and proce-  
25 dures that shall be established to require that active  
26 defense techniques are adequately coordinated to en-

1       sure that active defense techniques do not impede  
2       agency operations and mission delivery, threat re-  
3       sponse efforts, criminal investigations, and national  
4       security activities, including intelligence collection;  
5       and

6               (4) the development of a framework for the use  
7       of different active defense techniques by agencies.

8       **SEC. 303. SECURITY OPERATIONS CENTER AS A SERVICE**  
9               **PILOT.**

10       (a) **PURPOSE.**—The purpose of this section is for the  
11       Director of the Cybersecurity and Infrastructure Security  
12       Agency to run a security operation center on behalf of the  
13       head of another agency, alleviating the need to duplicate  
14       this function at every agency, and empowering a greater  
15       centralized cybersecurity capability.

16       (b) **PLAN.**—Not later than 1 year after the date of  
17       the enactment of this Act, the Director of the Cybersecu-  
18       rity and Infrastructure Security Agency shall develop a  
19       plan to establish a centralized Federal security operations  
20       center shared service offering within the Cybersecurity  
21       and Infrastructure Security Agency.

22       (c) **CONTENTS.**—The plan required under subsection  
23       (b) shall include considerations for—

24               (1) collecting, organizing, and analyzing agency  
25       information system data in real time;

1 (2) staffing and resources; and

2 (3) appropriate interagency agreements, con-  
3 cepts of operations, and governance plans.

4 (d) PILOT PROGRAM.—

5 (1) IN GENERAL.—Not later than 180 days  
6 after the date on which the plan required under sub-  
7 section (b) is developed, the Director of the Cyberse-  
8 curity and Infrastructure Security Agency, in con-  
9 sultation with the Director of the Office of Manage-  
10 ment and Budget, shall enter into a 1-year agree-  
11 ment with not less than 2 agencies to offer a secu-  
12 rity operations center as a shared service.

13 (2) ADDITIONAL AGREEMENTS.—After the date  
14 on which the briefing required under subsection  
15 (e)(1) is provided, the Director of the Cybersecurity  
16 and Infrastructure Security Agency, in consultation  
17 with the Director of the Office of Management and  
18 Budget, may enter into additional 1-year agreements  
19 described in paragraph (1) with agencies.

20 (e) BRIEFING AND REPORT.—

21 (1) BRIEFING.—Not later than 270 days after  
22 the date of the enactment of this Act, the Director  
23 of the Cybersecurity and Infrastructure Security  
24 Agency shall provide to appropriate congressional  
25 committees a briefing on the parameters of any 1-

1 year agreements entered into under subsection  
2 (d)(1).

3 (2) REPORT.—Not later than 90 days after the  
4 date on which the first 1-year agreement entered  
5 into under subsection (d) expires, the Director of the  
6 Cybersecurity and Infrastructure Security Agency  
7 shall submit to appropriate congressional committees  
8 a report on—

9 (A) the agreement; and

10 (B) any additional agreements entered into  
11 with agencies under subsection (d).

12 **SEC. 304. ENDPOINT DETECTION AND RESPONSE AS A**  
13 **SERVICE PILOT.**

14 (a) PURPOSE.—The Cybersecurity and Infrastruc-  
15 ture Security Agency is directed to establish and conduct  
16 a pilot to determine the feasibility, value, and efficacy of  
17 providing endpoint detection and response capabilities as  
18 a shared service to Federal agencies to reduce costs, en-  
19 hance interoperability, and continuously detect and miti-  
20 gate threat activity on Federal networks.

21 (b) PLAN.—Not later than 90 days after the date of  
22 the enactment of this Act, the Director of the Cybersecu-  
23 rity and Infrastructure Security Agency shall develop a  
24 plan to establish a centralized endpoint detection and re-

1 sponse shared service offering within the Cybersecurity  
2 and Infrastructure Security Agency.

3 (c) CONTENTS.—The plan required under subsection  
4 (b) shall include considerations for—

5 (1) understanding and assessing the full extent  
6 of endpoints across the Federal civilian environment;

7 (2) maximizing the value of existing agency in-  
8 vestments in endpoint detection and response tools  
9 and services;

10 (3) aggregating the available contract vehicles  
11 and options that provide agencies with appropriate  
12 capability for their environment and architecture;

13 (4) equipping all endpoints and services of pilot  
14 agencies with endpoint detection and response pro-  
15 grams;

16 (5) aggregating network, cloud, and endpoint  
17 data from both within the agency and across agen-  
18 cies to provide enterprise-wide monitoring of the net-  
19 work to detect abnormal network behavior and auto-  
20 mate defensive capabilities; and

21 (6) appropriate interagency agreements, con-  
22 cepts of operations, and governance plans.

23 (d) PILOT PROGRAM.—

24 (1) IN GENERAL.—Not later than 180 days  
25 after the date on which the plan required under sub-

1 section (b) is developed, the Director of the Cyberse-  
2 curity and Infrastructure Security Agency, in con-  
3 sultation with the Director, shall enter into a 1-year  
4 agreement with not less than 2 agencies to offer  
5 endpoint detection and response as a shared service.

6 (2) ADDITIONAL AGREEMENTS.—After the date  
7 on which the briefing required under subsection  
8 (e)(1) is provided, the Director of the Cybersecurity  
9 and Infrastructure Security Agency, in consultation  
10 with the Director, may enter into additional 1-year  
11 agreements described in paragraph (1) with agen-  
12 cies.

13 (e) BRIEFING AND REPORT.—

14 (1) BRIEFING.—Not later than 270 days after  
15 the date of the enactment of this Act, the Director  
16 of the Cybersecurity and Infrastructure Security  
17 Agency shall provide to the Committee on Homeland  
18 Security and Governmental Affairs of the Senate  
19 and the Committee on Homeland Security and the  
20 Committee on Oversight and Reform of the House  
21 of Representatives a briefing on the parameters of  
22 any 1-year agreements entered into under subsection  
23 (d)(1).

24 (2) REPORT.—Not later than 90 days after the  
25 date on which the first 1-year agreement entered

1 into under subsection (d) expires, the Director of the  
2 Cybersecurity and Infrastructure Security Agency  
3 shall submit to the Committee on Homeland Secu-  
4 rity and Governmental Affairs of the Senate and the  
5 Committee on Homeland Security and the Com-  
6 mittee on Oversight and Reform of the House of  
7 Representatives a report on—  
8 (A) the agreement; and  
9 (B) any additional agreements entered into  
10 with agencies under subsection (d).

○