

[DISCUSSION DRAFT]

117TH CONGRESS
2^D SESSION

H. R. _____

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

M____, _____ introduced the following bill; which was referred to the
Committee on _____

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”.

6 **SEC. 2. TABLE OF CONTENTS.**

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

- Sec. 1. Short title.
- Sec. 2. Table of contents.

Sec. 3. Definitions.

TITLE I—UPDATES TO FISMA

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

TITLE II—IMPROVING FEDERAL CYBERSECURITY

- Sec. 201. Mobile security standards.
- Sec. 202. Data and logging retention for incident response.
- Sec. 203. Federal penetration testing policy.
- Sec. 204. Ongoing threat hunting program.
- Sec. 205. Codifying vulnerability disclosure programs.
- Sec. 206. Implementing zero trust principles.
- Sec. 207. GAO automation report.
- Sec. 208. Extension of Federal Acquisition Security Council.
- Sec. 209. Federal chief information security officer.
- Sec. 210. Council of the inspectors general on integrity and efficiency dashboard.
- Sec. 211. Quantitative cybersecurity metrics.

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

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

1 **SEC. 3. DEFINITIONS.**

2 In this Act, unless otherwise specified:

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

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

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

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

6 (B) the Committee on Oversight and Re-
7 form of the House of Representatives; and

8 (C) the Committee on Homeland Security
9 of the House of Representatives.

10 (4) DIRECTOR.—The term “Director” means
11 the Director of the Office of Management and Budg-
12 et.

13 (5) INCIDENT.—The term “incident” has the
14 meaning given the term in section 3552(b) of title
15 44, United States Code.

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

20 (7) PENETRATION TEST.—The term “penetra-
21 tion test” has the meaning given the term in section
22 3552(b) of title 44, United States Code, as amended
23 by this Act.

24 (8) THREAT HUNTING.—The term “threat
25 hunting” means iteratively searching for threats to

1 systems that evade detection by automated threat
2 detection systems.

3 **TITLE I—UPDATES TO FISMA**

4 **SEC. 101. TITLE 44 AMENDMENTS.**

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

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

8 (A) by striking clause (v) and inserting the
9 following:

10 “(v) confidentiality, privacy, disclo-
11 sure, and sharing of information;”;

12 (B) by redesignating clause (vi) as clause
13 (vii); and

14 (C) by inserting after clause (v) the fol-
15 lowing:

16 “(vi) in consultation with the National
17 Cyber Director, security of information;
18 and”;

19 (2) in section 3505—

20 (A) in paragraph (2) of the first subsection
21 designated as subsection (c) by adding “dis-
22 covery of internet-accessible information sys-
23 tems and assets, as well as” after “an inventory
24 under this subsection shall include”;

1 (B) in paragraph (3) of the first subsection
2 designated as subsection (c)—

3 (i) in subparagraph (B)—

4 (I) by inserting “the Secretary of
5 Homeland Security acting through the
6 Director of the Cybersecurity and In-
7 frastructure Security Agency, the Na-
8 tional Cyber Director, and” before
9 “the Comptroller General”; and

10 (II) by striking “and” at the end;

11 (ii) in subparagraph (C)(v), by strik-
12 ing the period at the end and inserting “;
13 and”; and

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

16 “(D) maintained on a continual basis
17 through the use of automation, machine-read-
18 able data, and scanning wherever practicable.”;
19 and

20 (C) by striking the second subsection des-
21 ignated as subsection (c);

22 (3) in section 3506—

23 (A) in subsection (a)(3), by inserting “In
24 carrying out these duties, the Chief Information
25 Officer shall coordinate, as appropriate, with

1 the Chief Data Officer in accordance with the
2 designated functions under section 3520(e).”
3 after “reduction of information collection bur-
4 dens on the public.”;

5 (B) in subsection (b)(1)(C), by inserting “,
6 availability” after “integrity”;

7 (C) in subsection (g)—

8 (i) in paragraph (1), by striking
9 “and” at the end; and

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

12 and

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

15 (4) in section 3513—

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

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

20 “(c) Each agency providing a written plan under sub-
21 section (b) shall provide any portion of the written plan
22 addressing information security to the National Cyber Di-
23 rector.”.

24 (b) SUBCHAPTER II DEFINITIONS.—

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

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

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

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

14 (C) by inserting after paragraph (2), as so
15 redesignated, the following:

16 “(3) The term ‘high value asset’ means infor-
17 mation or an information system that the head of an
18 agency determines, using policies, principles, stand-
19 ards, or guidelines issued by the Director under sec-
20 tion 3553(a), to be so critical to the agency that the
21 loss or corruption of the information or the loss of
22 access to the information system would have a seri-
23 ous impact on the ability of the agency to perform
24 the mission of the agency or conduct business.”;

1 (D) by inserting after paragraph (7), as so
2 redesignated, the following:

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

6 (E) by inserting after paragraph (9), as so
7 redesignated, the following:

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

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

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

17 (2) CONFORMING AMENDMENTS.—

18 (A) HOMELAND SECURITY ACT OF 2002.—

19 Section 1001(c)(1)(A) of the Homeland Secu-
20 rity Act of 2002 (6 U.S.C. 511(1)(A)) is
21 amended by striking “section 3552(b)(5)” and
22 inserting “section 3552(b)”.

23 (B) TITLE 10.—

24 (i) SECTION 2222.—Section 2222(i)(8)
25 of title 10, United States Code, is amended

1 by striking “section 3552(b)(6)(A)” and
2 inserting “section 3552(b)(9)(A)”.

3 (ii) SECTION 2223.—Section
4 2223(c)(3) of title 10, United States Code,
5 is amended by striking “section
6 3552(b)(6)” and inserting “section
7 3552(b)”.

8 (iii) SECTION 2315.—Section 2315 of
9 title 10, United States Code, is amended
10 by striking “section 3552(b)(6)” and in-
11 sserting “section 3552(b)”.

12 (iv) SECTION 2339A.—Section
13 2339a(e)(5) of title 10, United States
14 Code, is amended by striking “section
15 3552(b)(6)” and inserting “section
16 3552(b)”.

17 (C) HIGH-PERFORMANCE COMPUTING ACT
18 OF 1991.—Section 207(a) of the High-Perform-
19 ance Computing Act of 1991 (15 U.S.C.
20 5527(a)) is amended by striking “section
21 3552(b)(6)(A)(i)” and inserting “section
22 3552(b)(9)(A)(i)”.

23 (D) INTERNET OF THINGS CYBERSECURITY
24 IMPROVEMENT ACT OF 2020.—Section 3(5)
25 of the Internet of Things Cybersecurity Im-

1 provement Act of 2020 (15 U.S.C. 278g–3a) is
2 amended by striking “section 3552(b)(6)” and
3 inserting “section 3552(b)”.

4 (E) NATIONAL DEFENSE AUTHORIZATION
5 ACT FOR FISCAL YEAR 2013.—Section
6 933(e)(1)(B) of the National Defense Author-
7 ization Act for Fiscal Year 2013 (10 U.S.C.
8 2224 note) is amended by striking “section
9 3542(b)(2)” and inserting “section 3552(b)”.

10 (F) IKE SKELTON NATIONAL DEFENSE AU-
11 THORIZATION ACT FOR FISCAL YEAR 2011.—The
12 Ike Skelton National Defense Authorization Act
13 for Fiscal Year 2011 (Public Law 111–383) is
14 amended—

15 (i) in section 806(e)(5) (10 U.S.C.
16 2304 note), by striking “section 3542(b)”
17 and inserting “section 3552(b)”;

18 (ii) in section 931(b)(3) (10 U.S.C.
19 2223 note), by striking “section
20 3542(b)(2)” and inserting “section
21 3552(b)”;

22 (iii) in section 932(b)(2) (10 U.S.C.
23 2224 note), by striking “section
24 3542(b)(2)” and inserting “section
25 3552(b)”.

1 (G) E-GOVERNMENT ACT OF 2002.—Sec-
2 tion 301(c)(1)(A) of the E-Government Act of
3 2002 (44 U.S.C. 3501 note) is amended by
4 striking “section 3542(b)(2)” and inserting
5 “section 3552(b)”.

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

10 (i) in subsection (a)(2), by striking
11 “section 3552(b)(5)” and inserting “sec-
12 tion 3552(b)”;

13 (ii) in subsection (f)—

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

17 (II) in paragraph (5), by striking
18 “section 3532(b)(2)” and inserting
19 “section 3552(b)”.

20 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II
21 of chapter 35 of title 44, United States Code, is amend-
22 ed—

23 (1) in section 3551—

1 (A) in paragraph (4), by striking “diag-
2 nose and improve” and inserting “integrate, de-
3 liver, diagnose, and improve”;

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

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

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

9 “(7) recognize that each agency has specific
10 mission requirements and, at times, unique cyberse-
11 curity requirements to meet the mission of the agen-
12 cy;

13 “(8) recognize that each agency does not have
14 the same resources to secure agency systems, and an
15 agency should not be expected to have the capability
16 to secure the systems of the agency from advanced
17 adversaries alone; and

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

21 (2) in section 3553—

22 (A) in subsection (a)—

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

1 (ii) in paragraph (6), by striking the
2 period at the end and inserting “; and”;
3 and

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

6 “(7) promoting, in consultation with the Direc-
7 tor of the Cybersecurity and Infrastructure Security
8 Agency, the National Cyber Director, and the Direc-
9 tor of the National Institute of Standards and Tech-
10 nology—

11 “(A) the use of automation to improve
12 Federal cybersecurity and visibility with respect
13 to the implementation of Federal cybersecurity;
14 and

15 “(B) the use of zero trust architecture
16 principles to improve resiliency and timely re-
17 sponse actions to incidents on Federal sys-
18 tems.”;

19 (B) in subsection (b)—

20 (i) in the matter preceding paragraph
21 (1), by striking “The Secretary, in con-
22 sultation with the Director” and inserting
23 “The Secretary of Homeland Security, act-
24 ing through the Director of the Cybersecu-
25 rity and Infrastructure Security Agency

1 and in consultation with the Director and
2 the National Cyber Director”;

3 (ii) in paragraph (2)(A), by inserting
4 “and reporting requirements under sub-
5 chapter IV of this chapter” after “section
6 3556”;

7 (iii) redesignate paragraphs (8) and
8 (9) as paragraphs (9) and (10); and

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

10 “(8) expeditiously seek opportunities to reduce
11 costs, administrative burdens, and other barriers to
12 information technology security and modernization
13 for Federal agencies, including through—

14 “(A) central shared services contracts for
15 cybersecurity capabilities identified as optimal
16 by the Director, in coordination with the Sec-
17 retary acting through the Director of the Cy-
18 bersecurity and Infrastructure Security Agency
19 and other agencies as appropriate; and

20 “(B) offering technical assistance and ex-
21 pertise to agencies on the selection and success-
22 ful engagement of highly adaptive cybersecurity
23 service contracts and other relevant contracts
24 provided by the U.S. General Services Adminis-
25 tration.”;

1 (C) in subsection (c)—

2 (i) in the matter preceding paragraph
3 (1), by striking “each year” and inserting
4 “each year during which agencies are re-
5 quired to submit reports under section
6 3554(c)” and by striking “preceding year”
7 and inserting “preceding two years”;

8 (ii) by striking paragraph (1);

9 (iii) by redesignating paragraphs (2),
10 (3), and (4) as paragraphs (1), (2), and
11 (3), respectively;

12 (iv) in paragraph (3), as so redesign-
13 dated, by striking “and” at the end; and

14 (v) by inserting after paragraph (3),
15 as so redesignated, the following:

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

18 (D) by redesignating subsections (i), (j),
19 (k), and (l) as subsections (j), (k), (l), and (m)
20 respectively;

21 (E) in subsection (h)—

22 (i) in paragraph (2), subparagraph
23 (A) adding “and the National Cyber Direc-
24 tor” after “in coordination with the Direc-
25 tor”;

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

4 (iii) in paragraph (3), subparagraph
5 (A), clause (iv) adding “, the National
6 Cyber Director,” after “the Secretary pro-
7 vides prior notice to the Director”;

8 (F) by inserting after subsection (h) the
9 following:

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

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

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

22 “(3) analysis of incident information under sec-
23 tion 3597;

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

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

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

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

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

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

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

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

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

18 “(1) the specific”;

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

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

24 “(2) the trends identified in the Federal risk
25 assessments performed under subsection (i).”; and

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

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

12 (3) in section 3554—

13 (A) in subsection (a)—

14 (i) in paragraph (1)—

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

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

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

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

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

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

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

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

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

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

1 “(III) information provided to
2 the agency through the vulnerability
3 disclosure program of the agency
4 under section 3559B;

5 “(IV) incidents; and

6 “(V) any other vulnerability in-
7 formation relating to agency systems
8 that is known to the agency;

9 “(vi) assess the impacts of potential
10 agency incidents to agency systems, data,
11 and operations based on the evaluations
12 described in clauses (ii) and (iv) and the
13 agency systems identified under clause
14 (iii); and

15 “(vii) assess the consequences of po-
16 tential incidents occurring on agency sys-
17 tems that would impact systems at other
18 agencies, including due to interconnectivity
19 between different agency systems or oper-
20 ational reliance on the operations of the
21 system or data in the system;”;

22 (III) in subparagraph (B), as so
23 redesignated, in the matter preceding
24 clause (i), by striking “providing in-
25 formation” and inserting “using infor-

1 mation from the assessment con-
2 ducted under subparagraph (A), pro-
3 viding information”;

4 (IV) in subparagraph (C), as so
5 redesignated—

6 (aa) in clause (ii) by insert-
7 ing “binding” before “oper-
8 ational”; and

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

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

13 “(E) providing an update on the ongoing
14 and continuous assessment performed under
15 subparagraph (A)—

16 “(i) upon request, to the inspector
17 general of the agency or the Comptroller
18 General of the United States; and

19 “(ii) on a periodic basis, as deter-
20 mined by guidance issued by the Director
21 but not less frequently than every 2 years,
22 to—

23 “(I) the Director;

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

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

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

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

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

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

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

1 “(ii) the Director; and

2 “(iii) the National Cyber Director;

3 and

4 “(H) if the head of the agency determines
5 there is need for additional cybersecurity proce-
6 dures, ensuring that those additional cybersecu-
7 rity procedures are reflected in the budget re-
8 quest of the agency;”;

9 (ii) in paragraph (2)—

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

15 (II) in subparagraph (B)—

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

19 “(i) standards”; and

20 (bb) by adding at the end
21 the following:

22 “(ii) the evaluation performed under
23 paragraph (1)(F); and

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

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

7 (B) in subsection (b)—

8 (i) by striking paragraph (1) and in-
9 serting the following:

10 “(1) pursuant to subsection (a)(1)(A), per-
11 forming ongoing and continuous agency system risk
12 assessments, which may include using guidelines and
13 automated tools consistent with standards and
14 guidelines promulgated under section 11331 of title
15 40, as applicable;”;

16 (ii) in paragraph (2)(D)—

17 (I) by redesignating clauses (iii)
18 and (iv) as clauses (iv) and (v), re-
19 spectively;

20 (II) by inserting after clause (ii)
21 the following:

22 “(iii) binding operational directives
23 and emergency directives promulgated by
24 the Director of the Cybersecurity and In-

1 frastructure Security Agency under section
2 3553;” and

3 (III) in clause (iv), as so redesign-
4 nated, by striking “as determined by
5 the agency; and” and inserting “as
6 determined by the agency, considering
7 the agency risk assessment performed
8 under subsection (a)(1)(A).”;

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

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

15 (v) by inserting after paragraph (6)
16 the following:

17 “(7) a process for providing the status of every
18 remedial action, as well as unremediated identified
19 system vulnerabilities, to the Director and the Direc-
20 tor of the Cybersecurity and Infrastructure Security
21 Agency, using automation and machine-readable
22 data to the greatest extent practicable;” and

23 (vi) in paragraph (8)(C), as so redesi-
24 gnated—

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

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

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

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

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

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

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

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

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

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

25 (C) in subsection (c)—

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

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

5 “(1) BIENNIAL REPORT.—Not later than 2
6 years after the date of the enactment of the Federal
7 Information Security Modernization Act of 2022 and
8 not less frequently than once every 2 years there-
9 after, using the continuous and ongoing agency sys-
10 tem risk assessment under subsection (a)(1)(A), the
11 head of each agency shall submit to the Director,
12 the Director of the Cybersecurity and Infrastructure
13 Security Agency, the majority and minority leaders
14 of the Senate, the Speaker and minority leader of
15 the House of Representatives, the Committee on
16 Homeland Security and Governmental Affairs of the
17 Senate, the Committee on Oversight and Reform of
18 the House of Representatives, the Committee on
19 Homeland Security of the House of Representatives,
20 the Committee on Commerce, Science, and Trans-
21 portation of the Senate, the Committee on Science,
22 Space, and Technology of the House of Representa-
23 tives, the appropriate authorization and appropria-
24 tions committees of Congress, the National Cyber

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

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

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

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

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

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

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

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

8 “(B) may include a classified annex.

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

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

20 (iii) in paragraph (5), as so redesign-
21 nated, by inserting “, including the report-
22 ing procedures established under section
23 11315(d) of title 40 and subsection
24 (a)(3)(A)(v) of this section,” after “poli-
25 cies, procedures, and practices”; and

1 (4) in section 3555—

2 (A) in the section heading, by striking
3 “**ANNUAL INDEPENDENT**” and inserting
4 “**INDEPENDENT**”;

5 (B) in subsection (a)—

6 (i) in paragraph (1), by inserting
7 “during which a report is required to be
8 submitted under section 3553(c),” after
9 “Each year”;

10 (ii) in paragraph (2)(A), by inserting
11 “, including by penetration testing and
12 analyzing the vulnerability disclosure pro-
13 gram of the agency” after “information
14 systems”; and

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

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

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

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

1 (E) by striking subsection (f) and inserting
2 the following:

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

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

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

17 “(A) specific information system incidents; or

18 “(B) specific information system
19 vulnerabilities.”;

20 (F) in subsection (g)(2)—

21 (i) by striking “this subsection shall”

22 and inserting “this subsection—

23 “(A) shall”;

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

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

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

9 (G) striking subsection (j); and
10 (5) in section 3556(a)(4) by striking “3554(b)”
11 and inserting “3554(a)(1)(A)”.

12 (d) CONFORMING AMENDMENTS.—

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

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

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

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

“3555. Independent evaluation.”.

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

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

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

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

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

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

21 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

1 “SUBCHAPTER IV—FEDERAL SYSTEM
2 INCIDENT RESPONSE

3 “§ 3591. Definitions

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

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

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

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

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

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

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

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

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

23 “(G) the Director;

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

1 “(I) the National Cyber Director;

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

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

6 “(2) AWARDEE.—The term ‘awardee’—

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

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

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

16 “(4) CONTRACTOR.—The term ‘contractor’
17 means a prime contractor of an agency or a subcon-
18 tractor of a prime contractor of an agency.

19 “(5) FEDERAL INFORMATION.—The term ‘Fed-
20 eral information’ means information created, col-
21 lected, processed, maintained, disseminated, dis-
22 closed, or disposed of by or for the Federal Govern-
23 ment in any medium or form.

24 “(6) FEDERAL INFORMATION SYSTEM.—The
25 term ‘Federal information system’ means an infor-

1 information system used or operated by an agency, a con-
2 tractor, or another organization on behalf of an
3 agency.

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

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

13 “(9) VULNERABILITY DISCLOSURE.—The term
14 ‘vulnerability disclosure’ means a vulnerability iden-
15 tified under section 3559B.

16 **“§ 3592. Notification of breach**

17 “(a) NOTIFICATION.—As expeditiously as practicable
18 and without unreasonable delay, and in any case not later
19 than 45 days after an agency has a reasonable basis to
20 conclude that a breach has occurred, the head of the agen-
21 cy, in consultation with the chief privacy officer of the
22 agency, shall—

23 “(1) determine whether notice to any individual
24 potentially affected by the breach is appropriate

1 based on an assessment of the risk of harm to the
2 individual that considers—

3 “(A) the nature and sensitivity of the per-
4 sonally identifiable information affected by the
5 breach;

6 “(B) the likelihood of access to and use of
7 the personally identifiable information affected
8 by the breach;

9 “(C) the type of breach; and

10 “(D) any other factors determined by the
11 Director; and

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

15 “(A) to the last known mailing address of
16 the individual; or

17 “(B) through an appropriate alternative
18 method of notification that the head of the
19 agency or a designated senior-level individual of
20 the agency selects based on factors determined
21 by the Director.

22 “(b) CONTENTS OF NOTICE.—Each notice of a
23 breach provided to an individual under subsection (a)(2)
24 shall include—

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

1 “(2) if possible, a description of the types of
2 personally identifiable information affected by the
3 breach;

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

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

8 “(B) may include a telephone number,
9 mailing address, or a website;

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

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

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

21 “(c) DELAY OF NOTIFICATION.—

22 “(1) IN GENERAL.—The Attorney General, the
23 Director of National Intelligence, or the Secretary of
24 Homeland Security may delay a notification required
25 under subsection (a) if the notification would—

1 “(A) impede a criminal investigation or a
2 national security activity;

3 “(B) reveal sensitive sources and methods;

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

5 “(D) hamper security remediation actions.

6 “(2) DOCUMENTATION.—

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

16 “(B) CONTENTS.—A report required under
17 subparagraph (A) shall include a written state-
18 ment from the entity that delayed the notifica-
19 tion explaining the need for the delay.

20 “(C) FORM.—The report required under
21 subparagraph (A) shall be unclassified but may
22 include a classified annex.

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

1 “(d) UPDATE NOTIFICATION.—If an agency deter-
2 mines there is a significant change in the reasonable basis
3 to conclude that a breach occurred, a significant change
4 to the determination made under subsection (a)(1), or that
5 it is necessary to update the details of the information pro-
6 vided to potentially affected individuals as described in
7 subsection (b), the agency shall as expeditiously as prac-
8 ticable and without unreasonable delay, and in any case
9 not later than 30 days after such a determination, notify
10 each individual who received a notification pursuant to
11 subsection (a) of those changes.

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

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

18 “(2) the Director from issuing guidance relat-
19 ing to notifications of major incidents or the head of
20 an agency from providing more information than de-
21 scribed in subsection (b) when notifying individuals
22 potentially affected by breaches.

23 **“§ 3593. Congressional and executive branch reports**

24 “(a) INITIAL REPORT.—

1 “(1) IN GENERAL.—Not later than 72 hours
2 after an agency has a reasonable basis to conclude
3 that a major incident occurred, the head of the
4 agency impacted by the major incident shall submit
5 to the appropriate reporting entities a written re-
6 port. Within 7 days of a major incident determina-
7 tion, the head of the agency impacted shall coordi-
8 nate with the National Cyber Director, or their des-
9 ignee, to provide a briefing, along with any other
10 Federal entity determined appropriate by the Na-
11 tional Cyber Director, to the Committee on Home-
12 land Security and Governmental Affairs of the Sen-
13 ate, the Committee on Oversight and Reform of the
14 House of Representatives, the Committee on Home-
15 land Security of the House of Representatives, and
16 the appropriate authorization and appropriations
17 committees of Congress, in the manner requested by
18 the Congressional entities, taking into account—

19 “(A) the information known at the time of
20 the report, including the threat having likely
21 caused the major incident;

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

24 “(C) the classification level of the informa-
25 tion contained in the report.

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

7 “(A) a summary of the information avail-
8 able about the major incident, including how
9 the major incident occurred and, if applicable,
10 information relating to the major incident as a
11 breach, based on information available to agen-
12 cy officials as of the date on which the agency
13 submits the report;

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

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

24 “(3) COMPONENTS OF BRIEFING.—The 7 day
25 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) ANNUAL REPORT.—Each agency shall submit as
25 part of the annual report required under section

1 3554(c)(1) of this title a description of each major inci-
2 dent that occurred during the 1-year period preceding the
3 date on which the annual 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 DELIVERY.—Any written report re-
14 quired to be submitted under this section may be sub-
15 mitted in a paper or electronic format.

16 “(g) RULE OF CONSTRUCTION.—Nothing in this sec-
17 tion shall be construed to limit—

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

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

23 **“§ 3594. Government information sharing and inci-**
24 **dent response**

25 “(a) IN GENERAL.—

1 “(1) INCIDENT REPORTING.—Subject to limita-
2 tions in subsection (b), the head of each agency shall
3 provide any information relating to any incident af-
4 fecting their agency, whether the information is ob-
5 tained by the Federal Government directly or indi-
6 rectly, to the Cybersecurity and Infrastructure Secu-
7 rity Agency, the Office of Management and Budget,
8 and the Office of the National Cyber Director.

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 share in-
13 formation relating to an incident with any agencies
14 that may be impacted by the incident, or are poten-
15 tially susceptible or similarly targeted.

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

1 “(b) COMPLIANCE.—The information provided under
2 subsection (a) shall take into account the level of classi-
3 fication of the information and any information sharing
4 limitations and protections, such as limitations and protec-
5 tions relating to law enforcement, national security, pri-
6 vacy, statistical confidentiality, or other factors deter-
7 mined by the Director.

8 “(c) INCIDENT RESPONSE.—Each agency that has a
9 reasonable basis to conclude that a major incident oc-
10 curred involving Federal information in electronic medium
11 or form, as defined by the Director and not involving a
12 national security system, regardless of delays from notifi-
13 cation granted for a major incident, shall coordinate with
14 the Cybersecurity and Infrastructure Security Agency to
15 facilitate asset response activities and recommendations
16 for mitigating future incidents, and with the Federal Bu-
17 reau of Investigation to facilitate threat response activi-
18 ties, consistent with relevant policies, principles, stand-
19 ards, and guidelines on information security.

20 **“§ 3595. Responsibilities of contractors and awardees**

21 “(a) REPORTING.—

22 “(1) IN GENERAL.—Unless otherwise specified
23 in a contract, grant, cooperative agreement, or any
24 other transaction agreement, any contractor or
25 awardee of an agency shall report to the agency

1 within the same amount of time such agency is re-
2 quired to report an incident to the Cybersecurity
3 and Infrastructure Security Agency, if the con-
4 tractor or awardee has a reasonable basis to suspect
5 or conclude that—

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

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

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

24 “(2) PROCEDURES.—

1 “(A) MAJOR INCIDENT.—Following a re-
2 port of a breach or major incident by a con-
3 tractor or awardee under paragraph (1), the
4 agency, in consultation with the contractor or
5 awardee, shall carry out the requirements under
6 sections 3592, 3593, and 3594 with respect to
7 the major incident.

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

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

19 **“§ 3596. Training**

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

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

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

6 “(2) the obligation of a covered individual to re-
7 port to the agency a confirmed major incident and
8 any suspected incident involving information in any
9 medium or form, including paper, oral, and elec-
10 tronic.

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

15 **“§ 3597. Analysis and report on Federal incidents**

16 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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

1 “(i) attacker tactics, techniques, and
2 procedures; and

3 “(ii) system vulnerabilities, including
4 zero day exploitations, unpatched systems,
5 and information system misconfigurations;

6 “(B) the scope and scale of incidents at
7 agencies;

8 “(C) common root causes of incidents
9 across multiple agencies;

10 “(D) agency incident response, recovery,
11 and remediation actions and the effectiveness of
12 those actions, as applicable;

13 “(E) lessons learned and recommendations
14 in responding to, recovering from, remediating,
15 and mitigating future incidents; and

16 “(F) trends across multiple Federal agen-
17 cies to address intrusion detection and incident
18 response capabilities using the metrics estab-
19 lished under section 224(c) of the Cybersecurity
20 Act of 2015 (6 U.S.C. 1522(c)).

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

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

1 “(A) IN GENERAL.—The Director shall
2 share on an ongoing basis the analyses required
3 under this subsection with agencies and the Na-
4 tional Cyber Director to—

5 “(i) improve the understanding of cy-
6 bersecurity risk of agencies; and

7 “(ii) support the cybersecurity im-
8 provement efforts of agencies.

9 “(B) FORMAT.—In carrying out subpara-
10 graph (A), the Director shall share the anal-
11 yses—

12 “(i) in human-readable written prod-
13 ucts; and

14 “(ii) to the greatest extent practicable,
15 in machine-readable formats in order to
16 enable automated intake and use by agen-
17 cies.

18 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—
19 Not later than 2 years after the date of the enactment
20 of this section, and not less frequently than annually
21 thereafter, the Director of the Cybersecurity and Infra-
22 structure Security Agency, in consultation with the Direc-
23 tor, the National Cyber Director, and the heads of other
24 agencies as appropriate, shall submit to the appropriate
25 reporting entities a report that includes—

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

4 “(2) the quantitative and qualitative analyses of
5 incidents developed under subsection (a)(1) on an
6 agency-by-agency basis and comprehensively across
7 the Federal Government, including—

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

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

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

14 “(A) a description of each major incident;
15 and

16 “(B) an analysis of the agency’s perform-
17 ance against the metrics established under sec-
18 tion 224(c) of the Cybersecurity Act of 2015 (6
19 U.S.C. 1522(c)).

20 “(c) PUBLICATION.—To the extent that publication
21 is consistent with national security interests, a version of
22 each report submitted under subsection (b) shall be made
23 publicly available on the website of the Cybersecurity and
24 Infrastructure Security Agency during the year in which
25 the report is submitted.

1 “(d) INFORMATION PROVIDED BY AGENCIES.—

2 “(1) IN GENERAL.—The analysis required
3 under subsection (a) and each report submitted
4 under subsection (b) shall use information provided
5 by agencies under section 3594(a).

6 “(2) NATIONAL SECURITY SYSTEM REPORTS.—

7 “(A) IN GENERAL.—Annually, the head of
8 an agency that operates or exercises control of
9 a national security system shall submit a report
10 that includes the information described in sub-
11 section (b) with respect to the agency to the ex-
12 tent that the submission is consistent with
13 standards and guidelines for national security
14 systems issued in accordance with law and as
15 directed by the President to—

16 “(i) the majority and minority leaders
17 of the Senate,

18 “(ii) the Speaker and minority leader
19 of the House of Representatives;

20 “(iii) the Committee on Homeland Se-
21 curity and Governmental Affairs of the
22 Senate;

23 “(iv) the Select Committee on Intel-
24 ligence of the Senate;

1 “(v) the Committee on Armed Serv-
2 ices of the Senate;

3 “(vi) the Committee on Appropria-
4 tions of the Senate;

5 “(vii) the Committee on Oversight and
6 Reform of the House of Representatives;

7 “(viii) the Committee on Homeland
8 Security of the House of Representatives;

9 “(ix) the Permanent Select Committee
10 on Intelligence of the House of Represent-
11 atives;

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

14 “(xi) the Committee on Appropria-
15 tions of the House of Representatives.

16 “(B) CLASSIFIED FORM.—A report re-
17 quired under subparagraph (A) may be sub-
18 mitted in a classified form.

19 “(e) REQUIREMENT FOR COMPILING INFORMA-
20 TION.—In publishing the public report required under
21 subsection (c), the Director of the Cybersecurity and In-
22 frastructure Security Agency shall sufficiently compile in-
23 formation such that no specific incident of an agency can
24 be identified, except with the concurrence of the Director
25 of the Office of Management and Budget, the National

1 Cyber Director, and in consultation with the impacted
2 agency.

3 **“§ 3598. Major incident definition**

4 “(a) IN GENERAL.—Not later than 180 days after
5 the date of the enactment of the Federal Information Se-
6 curity Modernization Act of 2022, the Director, in coordi-
7 nation with the Director of the Cybersecurity and Infra-
8 structure Security Agency and the National Cyber Direc-
9 tor, shall develop and promulgate guidance on the defini-
10 tion of the term ‘major incident’ for the purposes of sub-
11 chapter II and this subchapter.

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

15 “(1) include, with respect to any information
16 collected or maintained by or on behalf of an agency
17 or an information system used or operated by an
18 agency or by a contractor of an agency or another
19 organization on behalf of an agency—

20 “(A) any incident the head of the agency
21 determines is likely to result in demonstrable
22 harm to—

23 “(i) the national security interests,
24 foreign relations or the economy of the
25 United States; or

1 “(ii) the public confidence, civil lib-
2 erties, or public health and safety of the
3 people of the United States;

4 “(B) any incident the head of the agency
5 determines may have a significant impact on
6 the confidentiality, integrity, or availability of a
7 high value asset; and

8 “(C) any other type of incident determined
9 appropriate by the Director; and

10 “(2) stipulate that the Director, in coordination
11 with the National Cyber Director, shall declare a
12 major incident at each agency impacted by an inci-
13 dent if it is determined that an incident—

14 “(A) occurs at not less than 2 agencies;
15 and

16 “(B) is enabled by—

17 “(i) a common technical root cause,
18 such as a supply chain compromise or a
19 common software or hardware vulner-
20 ability; or

21 “(ii) the related activities of a com-
22 mon threat actor.

23 “(c) EVALUATION AND UPDATES.—Not later than 2
24 years after the date of the enactment of the Federal Infor-
25 mation Security Modernization Act of 2022, and not less

1 frequently than every 2 years thereafter, the Director shall
2 submit to the Committee on Homeland Security and Gov-
3 ernmental Affairs of the Senate and the Committee on
4 Oversight and Reform of the House of Representatives an
5 evaluation, which shall include—

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

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

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

13 (2) CLERICAL AMENDMENT.—The table of sec-
14 tions for chapter 35 of title 44, United States Code,
15 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.”.

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

17 (a) MODERNIZING GOVERNMENT TECHNOLOGY.—

18 Subtitle G of title X of Division A of the National Defense
19 Authorization Act for Fiscal Year 2018 (Public Law 115–
20 91; 40 U.S.C. 11301 note) is amended in section 1078—

1 (1) by striking subsection (a) and inserting the
2 following:

3 “(a) DEFINITIONS.—In this section:

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

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

10 (2) in subsection (c)—

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

14 (B) in paragraph (5)—

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

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

19 and

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

22 “(C) a senior official from the Cybersecu-
23 rity and Infrastructure Security Agency of the
24 Department of Homeland Security, appointed
25 by the Director.”; and

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

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

6 (1) in section 11302—

7 (A) in subsection (b), by striking “use, se-
8 curity, and disposal of” and inserting “use, and
9 disposal of, and, in consultation with the Direc-
10 tor of the Cybersecurity and Infrastructure Se-
11 curity Agency and the National Cyber Director,
12 promote and improve the security of,”;

13 (B) in subsection (c)(3)(B), by adding at
14 the end the following:

15 “(iii) The Director may make avail-
16 able, upon request, to the National Cyber
17 Director any cybersecurity funding infor-
18 mation described in subparagraph (A)(ii)
19 that is provided to the Director under
20 clause (ii) of this subparagraph.”;

21 (C) in subsection (f), by striking “The Di-
22 rector shall” and inserting “The Director
23 shall—

24 “(1) encourage the heads of the executive agen-
25 cies to develop and use the best practices in the ac-

1 quisition of information technology, including supply
2 chain security best practices; and

3 “(2) consult with the Federal Chief Information
4 Security Officer appointed by the President under
5 section 3607 of title 44, United States Code, for the
6 development and use of supply chain security best
7 practices.”; and

8 (D) in subsection (h), by inserting “, in-
9 cluding cybersecurity performances,” after “the
10 performances”; and

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

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

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

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

17 “(iii) whether the function should be
18 performed by a shared service offered by
19 another executive agency.”.

20 (c) SUBCHAPTER II.—Subchapter II of chapter 113
21 of subtitle III of title 40, United States Code, is amend-
22 ed—

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

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

4 (3) in section 11315, by adding at the end the
5 following:

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

9 “(1) the Chief Information Officer designated
10 under section 3506(a)(2) of title 44 or an equivalent
11 official of the agency of which the component agency
12 is a component; and

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

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

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

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

21 (1) in subsection (a), by striking “section
22 3532(b)(1)” and inserting “section 3552(b)”;

23 (2) in subsection (b)(1)(A), by striking “the
24 Secretary of Homeland Security” and inserting “the

1 Director of the Cybersecurity and Infrastructure Se-
2 curity Agency”;

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

4 “(e) REVIEW OF OFFICE OF MANAGEMENT AND
5 BUDGET GUIDANCE AND POLICY.—

6 “(1) CONDUCT OF REVIEW.—

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

23 “(B) FEDERAL RISK ASSESSMENTS.—In
24 conducting the review described in subpara-
25 graph (A), the Director shall consider the Fed-

1 eral risk assessments performed under section
2 3553(i) of title 44.

3 “(C) REQUIREMENTS BURDEN REDUCTION
4 AND CLARITY.—In conducting the review de-
5 scribed in subparagraph (A), the Director shall
6 consider the cumulative reporting and compli-
7 ance burden to agencies as well as the clarity
8 of the requirements and deadlines contained in
9 guidance and policy documents.

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

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

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

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

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

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

1 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**
2 **SPONSE.**

3 (a) RESPONSIBILITIES OF THE CYBERSECURITY AND
4 INFRASTRUCTURE SECURITY AGENCY.—

5 (1) IN GENERAL.—Not later than 180 days
6 after the date of the enactment of this Act, the Di-
7 rector of the Cybersecurity and Infrastructure Secu-
8 rity Agency shall—

9 (A) develop a plan for the development of
10 the analysis required under section 3597(a) of
11 title 44, United States Code, as added by this
12 Act, and the report required under subsection
13 (b) of that section that includes—

14 (i) a description of any challenges the
15 Director anticipates encountering; and

16 (ii) the use of automation and ma-
17 chine-readable formats for collecting, com-
18 piling, monitoring, and analyzing data; and

19 (B) provide to the appropriate congres-
20 sional committees a briefing on the plan devel-
21 oped under subparagraph (A).

22 (2) BRIEFING.—Not later than 1 year after the
23 date of the enactment of this Act, the Director of
24 the Cybersecurity and Infrastructure Security Agen-
25 cy shall provide to the appropriate congressional
26 committees a briefing on—

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

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

6 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
7 OFFICE OF MANAGEMENT AND BUDGET.—

8 (1) 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 (2) 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 (3) 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 (4) 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 (5) 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 to investigate potential criminal
23 activity; and

24 (6) requirements to ensure that, subject to com-
25 pliance with statistical laws and other relevant data

1 protection requirements, the highest level security
2 operations center of each agency has visibility into
3 all agency logs.

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

14 (d) SUNSET.—This section will cease to be in effect
15 on the date that is 10 years after the date of enactment
16 of this Act.

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

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

21 **“§ 3559A. Federal penetration testing**

22 “(a) GUIDANCE.—

23 “(1) IN GENERAL.—The Director shall, in con-
24 sultation with the Secretary of the Department of

1 Homeland Security, issue guidance to agencies
2 that—

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

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

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

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

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

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

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

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

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

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

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

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

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

“3559A. Federal penetration testing.”.

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

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

3 (2) by redesignating paragraph (9) as para-
4 graph (10); and

5 (3) by inserting after paragraph (8) the fol-
6 lowing:

7 “(9) performing penetration testing to identify
8 vulnerabilities within Federal information systems;
9 and”.

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

11 (a) **THREAT HUNTING PROGRAM.**—

12 (1) **IN GENERAL.**—Not later than 540 days
13 after the date of the enactment of this Act, the Di-
14 rector of the Cybersecurity and Infrastructure Secu-
15 rity Agency shall, in accordance with the authorities
16 granted the Secretary under sections 3553(b)(7)-
17 (8) and 3553(m) of title 44, United States Code (as
18 redesignated by this Act), establish a program to
19 provide ongoing, hypothesis-driven threat-hunting
20 services on the network of each agency.

21 (2) **PLAN.**—Not later than 180 days after the
22 date of the enactment of this Act, the Director of
23 the Cybersecurity and Infrastructure Security Agen-
24 cy shall develop a plan to establish the program re-
25 quired under paragraph (1) that describes how the

1 Director of the Cybersecurity and Infrastructure Se-
2 curity Agency plans to—

3 (A) determine the method for collecting,
4 storing, accessing, analyzing, and safeguarding
5 appropriate agency data;

6 (B) provide on-premises support to agen-
7 cies;

8 (C) staff threat hunting services;

9 (D) allocate available human and financial
10 resources to implement the plan; and

11 (E) provide input to the heads of agencies
12 on the use of—

13 (i) more stringent standards under
14 section 11331(c)(1) of title 40, United
15 States Code; and

16 (ii) additional cybersecurity proce-
17 dures under section 3554 of title 44,
18 United States Code.

19 (b) REPORTS.—The Director of the Cybersecurity
20 and Infrastructure Security Agency, in consultation with
21 the Director, shall submit to the appropriate congressional
22 committees—

23 (1) not later than 30 days after the date on
24 which the Director of the Cybersecurity and Infra-
25 structure Security Agency completes the plan re-

1 quired under subsection (a)(2), a report on the plan
2 to provide threat hunting services to agencies;

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

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

16 **SEC. 205. CODIFYING VULNERABILITY DISCLOSURE PRO-**
17 **GRAMS.**

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

21 **“§ 3559B. Federal vulnerability disclosure programs**

22 “(a) DEFINITIONS.—In this section:

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

1 “(2) REPORTER.—The term ‘reporter’ means
2 an individual that submits a vulnerability report
3 pursuant to the vulnerability disclosure process of an
4 agency.

5 “(b) RESPONSIBILITIES OF OMB.—

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

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

16 “(B) is authorized under the vulnerability
17 disclosure policy of the agency developed under
18 subsection (d)(2).

19 “(2) SHARING INFORMATION WITH CISA.—The
20 Director of the Office of Management and Budget,
21 in coordination with the Director of the Cybersecu-
22 rity and Infrastructure Security Agency and in con-
23 sultation with the National Cyber Director, shall
24 issue guidance to agencies on sharing relevant infor-
25 mation in a consistent, automated, and machine

1 readable manner with the Director of the Cybersecu-
2 rity and Infrastructure Security Agency, including—

3 “(A) any valid or credible reports of newly
4 discovered or not publicly known vulnerabilities
5 (including misconfigurations) on Federal infor-
6 mation systems that use commercial software or
7 services;

8 “(B) information relating to vulnerability
9 disclosure, coordination, or remediation activi-
10 ties of an agency, particularly as those activities
11 relate to outside organizations—

12 “(i) with which the head of the agency
13 believes the Director of the Cybersecurity
14 and Infrastructure Security Agency can as-
15 sist; or

16 “(ii) about which the head of the
17 agency believes the Director of the Cyber-
18 security and Infrastructure Security Agen-
19 cy should know; and

20 “(C) any other information with respect to
21 which the head of the agency determines helpful
22 or necessary to involve the Director of the Cy-
23 bersecurity and Infrastructure Security Agency.

24 “(3) AGENCY VULNERABILITY DISCLOSURE
25 POLICIES.—The Director shall issue guidance to

1 agencies on the required minimum scope of agency
2 systems covered by the vulnerability disclosure policy
3 of an agency required under subsection (d)(2).

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

7 “(1) provide support to agencies with respect to
8 the implementation of the requirements of this sec-
9 tion;

10 “(2) develop tools, processes, and other mecha-
11 nisms determined appropriate to offer agencies capa-
12 bilities to implement the requirements of this sec-
13 tion; and

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

17 “(d) RESPONSIBILITIES OF AGENCIES.—

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

22 “(A) an appropriate security contact; and

23 “(B) the component of the agency that is
24 responsible for the internet accessible services
25 offered at the domain.

1 “(2) VULNERABILITY DISCLOSURE POLICY.—

2 The head of each agency shall develop and make
3 publicly available a vulnerability disclosure policy for
4 the agency, which shall—

5 “(A) describe—

6 “(i) the scope of the systems of the
7 agency included in the vulnerability disclo-
8 sure policy;

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

11 “(iii) the type of information system
12 testing that is not authorized by the agen-
13 cy; and

14 “(iv) the disclosure policy of the agen-
15 cy for sensitive information;

16 “(B) with respect to a report to an agency,
17 describe—

18 “(i) how the reporter should submit
19 the report; and

20 “(ii) if the report is not anonymous,
21 when the reporter should anticipate an ac-
22 knowledgment of receipt of the report by
23 the agency;

24 “(C) include any other relevant informa-
25 tion; and

1 “(D) be mature in scope, covering all inter-
2 net accessible Federal information systems used
3 or operated by that agency or on behalf of that
4 agency.

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

10 “(f) CONGRESSIONAL REPORTING.—Not later than
11 90 days after the date of the enactment of the Federal
12 Information Security Modernization Act of 2022, and an-
13 nually thereafter for a 3-year period, the Director of the
14 Cybersecurity and Infrastructure Security Agency, in con-
15 sultation with the Director, shall provide to the Committee
16 on Homeland Security and Governmental Affairs of the
17 Senate and the Committee on Oversight and Reform of
18 the House of Representatives a briefing on the status of
19 the use of vulnerability disclosure policies under this sec-
20 tion at agencies, including, with respect to the guidance
21 issued under subsection (b)(3), an identification of the
22 agencies that are compliant and not compliant.

23 “(g) EXEMPTIONS.—The authorities and functions of
24 the Director and Director of the Cybersecurity and Infra-

1 structure Security Agency under this section shall not
2 apply to national security systems.

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

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

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

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

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

“3559B. Federal vulnerability disclosure programs”.

18 **SEC. 206. IMPLEMENTING ZERO TRUST PRINCIPLES.**

19 (a) GUIDANCE.—The Director shall maintain guid-
20 ance on, and not later than 2 years after the date of the
21 enactment of this Act, provide an update to the appro-
22 priate congressional committees on progress in increasing
23 the internal defenses of agency systems through the adop-
24 tion of zero trust cybersecurity principles across the gov-
25 ernment, including—

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

4 (2) implementing principles of least privilege in
5 administering information security programs;

6 (3) limiting the ability of entities that cause in-
7 cidents to move laterally through or between agency
8 systems;

9 (4) identifying incidents quickly;

10 (5) isolating and removing unauthorized entities
11 from agency systems quickly;

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

14 (7) a summary of the agency progress reports
15 required under subsection (b).

16 (b) AGENCY PROGRESS REPORTS.—Not later than
17 270 days after the date of the enactment of this Act, the
18 head of each agency shall submit to the Director a
19 progress report on implementing an information security
20 program based on a zero trust cybersecurity strategy,
21 which shall include—

22 (1) a description of any steps the agency has
23 completed, including progress toward achieving any
24 requirements issued by the Director, including the
25 adoption of any models or reference architecture;

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

4 (3) a schedule to implement any planned activi-
5 ties.

6 **SEC. 207. GAO AUTOMATION REPORT.**

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

15 **SEC. 208. EXTENSION OF FEDERAL ACQUISITION SECURITY**
16 **COUNCIL.**

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

20 (b) **DESIGNATION.**—Section 1322(c)(1) of title 41,
21 United States Code, is amended by striking “Not later
22 than” and all that follows through the end of the para-
23 graph and inserting “ The Director of OMB shall des-
24 ignate the Federal Chief Information Security Officer ap-
25 pointed by the President under section 3607 of title 44,

1 United States Code, or an equivalent senior-level official
2 from the Office of Management and Budget if the position
3 is vacant, to serve as the Chairperson of the Council.”.

4 (c) DEFINITION.—Section 1321 of title 41, United
5 States Code, is amended by adding the following definition
6 and renumbering accordingly:

7 “(8) SOFTWARE BILL OF MATERIALS.—The
8 term ‘software bill of materials’ shall have the mean-
9 ing given to it by the Administrator of the National
10 Telecommunications and Information Administra-
11 tion.”.

12 (d) REQUIREMENT.—Subsection 1326(b) of title 41,
13 United States Code, is amended by inserting the following
14 paragraph before paragraph (6) and renumbering all sub-
15 sequent paragraphs accordingly:

16 “(6) maintaining an inventory of all available
17 Software Bills of Materials for each software prod-
18 ucts in use by the agency, as appropriate, to be
19 available to the Federal Acquisition Security Coun-
20 cil, the Secretary of Homeland Security acting
21 through the Director of Cybersecurity and Infra-
22 structure Security, and the National Cyber Direc-
23 tor.”.

1 **SEC. 209. FEDERAL CHIEF INFORMATION SECURITY OFFI-**
2 **CER.**

3 (a) IN GENERAL.—Chapter 36 of title 44, United
4 States Code, is amended by inserting at the end:

5 **“§ 3607. Federal chief information security officer**

6 “(a) ESTABLISHMENT.—There is established in the
7 Office of the Federal Chief Information Officer of the Of-
8 fice of Management and Budget a Federal Chief Informa-
9 tion Security Officer, who shall be appointed by the Presi-
10 dent.

11 “(b) DUTIES.—The Federal Chief Information Secu-
12 rity Officer shall report to the Federal Chief Information
13 Officer, and assist the Chief Information Officer in car-
14 rying out—

15 “(1) all functions under this chapter;

16 “(2) all functions assigned to the Director
17 under title II of the E-Government Act of 2002;

18 “(3) other electronic government initiatives,
19 consistent with other statutes; and

20 “(4) other initiatives determined by the Chief
21 Information Officer.

22 “(c) ADDITIONAL DUTIES.—The Federal Chief Infor-
23 mation Security Officer shall work with the Chief Informa-
24 tion Officer to oversee implementation of electronic Gov-
25 ernment under the E-Government Act of 2002, and other

1 relevant statutes, in a manner consistent with law, relating
2 to—

3 “(1) cybersecurity strategy, policy, and oper-
4 ations;

5 “(2) the development of enterprise architec-
6 tures;

7 “(3) information security;

8 “(4) privacy;

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

11 “(6) other areas of electronic Government as
12 determined by the Administrator.

13 “(d) ASSISTANCE.—The Federal Chief Information
14 Security Officer shall assist the Administrator in the per-
15 formance of electronic Government functions as described
16 in section 3602(f).”.

17 (b) IN GENERAL.—Section 1500 of title 6, United
18 States Code, is amended by adding:

19 “(d) DEPUTY DIRECTOR.—There shall be a Deputy
20 National Cyber Director for Agency Strategy, Capabilities,
21 and Budget, who shall be the Federal Chief Information
22 Security Officer appointed by the President under section
23 3607 of title 44, United States Code, and shall report to
24 the Director and assist the office in carrying out the fol-

1 lowing duties as it applies to the protection of Federal in-
2 formation systems by the agencies—

3 “(1) the preparation and oversight over the im-
4 plementation of the national cyber policy under sub-
5 section (c)(1)(C)(i);

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

9 “(3) reviewing annual budget proposals and
10 making related recommendations under subsection
11 (c)(1)(C)(iii); and

12 “(4) other initiatives determined by the Direc-
13 tor, or to be necessary to coordinate with the Office
14 by the Federal Chief Information Officer.”.

15 (c) CLERICAL AMENDMENT.—The table of sections
16 for chapter 36 of title 44, United States Code, is amended
17 by adding after the item relating to section 3606 the fol-
18 lowing:

“3607. Federal chief information security officer”.

19 **SEC. 210. COUNCIL OF THE INSPECTORS GENERAL ON IN-**
20 **TEGRITY AND EFFICIENCY DASHBOARD.**

21 Section 11(e)(2) of the Inspector General Act of 1978
22 (5 U.S.C. App.) is amended—

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

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. 211. 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,
19 shall—

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

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

25 (A) update the covered metrics; and

1 (B) establish new covered metrics.

2 (c) IMPLEMENTATION.—

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

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

18 (3) PENETRATION TESTS.—On not less than 2
19 occasions during the 2-year period following the date
20 on which guidance is promulgated under paragraph
21 (1), the Director shall ensure that not less than 3
22 agencies are subjected to substantially similar pene-
23 tration tests, as determined by the Director, in co-
24 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) CYBERSECURITY ACT OF 2015 UPDATES.—Sec-
23 tion 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522)
24 is amended—

1 (1) by amending subsection (c) to read as fol-
2 lows:

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

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

11 (3) by redesignating subsection (f) as sub-
12 section (e).

13 **TITLE III—PILOT PROGRAMS TO**
14 **ENHANCE FEDERAL CYBER-**
15 **SECURITY**

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

17 (a) DEFINITIONS.—In this section:

18 (1) APPROPRIATE CONGRESSIONAL COMMIT-
19 TEES.—The term “appropriate congressional com-
20 mittees” means—

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

24 (B) the Committee on Homeland Security,
25 the Committee on Oversight and Reform, and

1 the Committee on Appropriations of the House
2 of Representatives.

3 (2) INFORMATION TECHNOLOGY.—The term
4 “information technology”—

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

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

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

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

20 (B) that allocates resources based on the
21 risks identified and prioritized under subpara-
22 graph (A).

23 (b) ESTABLISHMENT OF RISK-BASED BUDGET
24 PILOT.—

25 (1) IN GENERAL.—

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

13 (B) CONTENTS OF PILOT.—The pilot re-
14 quired to be developed under paragraph (1)
15 shall—

16 (i) consider Federal and non-Federal
17 cyber threat intelligence products, where
18 available, to identify threats,
19 vulnerabilities, and risks;

20 (ii) consider the impact of agency op-
21 erations of compromise of systems, includ-
22 ing the interconnectivity to other agency
23 systems and the operations of other agen-
24 cies;

1 (iii) indicate where resources should
2 be allocated to have the greatest impact on
3 mitigating current and future threats and
4 current and future cybersecurity capabili-
5 ties;

6 (iv) be used to inform acquisition and
7 sustainment of—

8 (I) information technology and
9 cybersecurity tools;

10 (II) information technology and
11 cybersecurity architectures;

12 (III) information technology and
13 cybersecurity personnel; and

14 (IV) cybersecurity and informa-
15 tion technology concepts of operations;
16 and

17 (v) be used to evaluate and inform
18 government-wide cybersecurity programs of
19 the Department of Homeland Security.

20 (2) REPORTS.—Not later than 2 years after the
21 first publication of the budget submitted by the
22 President under section 1105 of title 31, United
23 States Code, following the date of the enactment of
24 this Act, the Director shall submit a report to Con-
25 gress on the implementation of the pilot for risk-

1 based budgeting for cybersecurity spending, an as-
2 sessment of agency implementation, and an evalua-
3 tion of whether the risk-based budget helps to miti-
4 gate cybersecurity vulnerabilities.

5 (3) GAO REPORT.—Not later than 3 years after
6 the date on which the first budget of the President
7 is submitted to Congress containing the validation
8 required under section 1105(a)(35)(A)(i)(V) of title
9 31, United States Code, as amended by subsection
10 (c), the Comptroller General of the United States
11 shall submit to the appropriate congressional com-
12 mittees a report that includes—

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

15 (B) an evaluation of whether the risk-
16 based budgets developed by pilot agencies are
17 effective at informing Federal Government-wide
18 cybersecurity programs; and

19 (C) any other information relating to risk-
20 based budgets the Comptroller General deter-
21 mines appropriate.

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

23 (a) DEFINITION.—In this section, the term “active
24 defense technique” has the meaning given in guidance

1 issued by the Director, in coordination with the Attorney
2 General.

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

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

13 (2) an evaluation of—

14 (A) the efficacy of a selection of active de-
15 fense techniques determined by the Director of
16 the Cybersecurity and Infrastructure Security
17 Agency; and

18 (B) factors that impact the efficacy of the
19 active defense techniques evaluated under sub-
20 paragraph (A);

21 (3) recommendations on safeguards and proce-
22 dures that shall be established to require that active
23 defense techniques are adequately coordinated to en-
24 sure that active defense techniques do not impede
25 agency operations and mission delivery, threat re-

1 sponse efforts, criminal investigations, and national
2 security activities, including intelligence collection;
3 and

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

6 **SEC. 303. SECURITY OPERATIONS CENTER AS A SERVICE**
7 **PILOT.**

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

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

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

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

24 (2) staffing and resources; and

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

3 (d) PILOT PROGRAM.—

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

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

19 (e) BRIEFING AND REPORT.—

20 (1) BRIEFING.—Not later than 260 days after
21 the date of the enactment of this Act, the Director
22 of the Cybersecurity and Infrastructure Security
23 Agency shall provide to appropriate congressional
24 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 **SHARED 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 60 days after the date of
22 enactment of this Act, the Director of the Cybersecurity
23 and Infrastructure Security Agency shall develop a plan
24 to establish a centralized endpoint detection and response

1 shared service offering within the Cybersecurity and Infra-
2 structure 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 endpoint data from both within
17 the agency and across agencies to provide enterprise-
18 wide monitoring of network to detect abnormal net-
19 work behavior; and

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

22 (d) PILOT PROGRAM.—

23 (1) IN GENERAL.—Not later than 60 days after
24 the date on which the plan required under sub-
25 section (b) is developed, the Director of the Cyberse-

1 security and Infrastructure Security Agency, in con-
2 sultation with the Director, shall enter into a 1-year
3 agreement with not less than 2 agencies to offer
4 endpoint detection and response as a shared service.

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

12 (e) BRIEFING AND REPORT.—

13 (1) BRIEFING.—Not later than 180 days after
14 the date of enactment of this Act, the Director of
15 the Cybersecurity and Infrastructure Security Agen-
16 cy shall provide to the Committee on Homeland Se-
17 curity and Governmental Affairs of the Senate and
18 the Committee on Homeland Security and the Com-
19 mittee on Oversight and Reform of the House of
20 Representatives a briefing on the parameters of any
21 1-year agreements entered into under subsection
22 (d)(1).

23 (2) REPORT.—Not later than 90 days after the
24 date on which the first 1-year agreement entered
25 into under subsection (d) expires, the Director of the

1 Cybersecurity and Infrastructure Security Agency
2 shall submit to the Committee on Homeland Secu-
3 rity and Governmental Affairs of the Senate and the
4 Committee on Homeland Security and the Com-
5 mittee on Oversight and Reform of the House of
6 Representatives a report on—

7 (A) the agreement; and

8 (B) any additional agreements entered into
9 with agencies under subsection (d).