



(Original Signature of Member)

117TH CONGRESS
2D 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

Mrs. CAROLYN B. MALONEY of New York (for herself and Mr. COMER) 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 architecture.
- Sec. 207. GAO automation report.
- Sec. 208. Extension of Federal Acquisition Security Council.
- Sec. 209. Federal chief information security officer.
- Sec. 210. Extension of Chief Data Officer Council.
- Sec. 211. Council of the inspectors general on integrity and efficiency dashboard.
- Sec. 212. 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 service pilot.

1 SEC. 3. DEFINITIONS.

2 In this Act, unless otherwise specified:

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

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

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

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

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

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

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

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

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

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

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

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

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

20 **TITLE I—UPDATES TO FISMA**

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

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

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

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

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

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

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

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

12 (2) in section 3505—

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

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

20 (i) in subparagraph (B)—

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

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

3 (II) by striking “and” at the end;

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

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

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

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

15 (3) in section 3506—

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

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

25 (4) in section 3513—

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

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

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

9 (b) SUBCHAPTER II DEFINITIONS.—

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

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

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

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

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

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

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

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

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

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

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

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

1 (2) CONFORMING AMENDMENTS.—

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

7 (B) TITLE 10.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

24 (ii) in subsection (f)—

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

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

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

10 (1) in section 3551—

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

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

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

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

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

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

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

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

6 (2) in section 3553—

7 (A) in subsection (a)—

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

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

12 and

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

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

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

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

4 (B) in subsection (b)—

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

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

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

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

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

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

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

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

11 (C) in subsection (c)—

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

18 (ii) by striking paragraph (1);

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

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

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

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

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

6 (E) in subsection (h)—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 “(1) IN GENERAL.—Not later than”;

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

7 “(A) the specific”;

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

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

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

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

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

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

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

5 (3) in section 3554—

6 (A) in subsection (a)—

7 (i) in paragraph (1)—

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

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

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

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

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

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

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

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

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

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

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

23 “(IV) incidents; and

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

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

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

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

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

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

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

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

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

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

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

18 “(I) the Director;

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

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

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

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

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

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

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

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

19 “(ii) the Director; and

20 “(iii) the National Cyber Director;
21 and

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

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

3 (ii) in paragraph (2)—

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

9 (II) in subparagraph (B)—

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

13 “(i) standards”; and

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

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

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

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

1 (B) in subsection (b)—

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

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

10 (ii) in paragraph (2)(D)—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (C) in subsection (c)—

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

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

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

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

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

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

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

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

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

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

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

23 “(B) may include a classified annex.

24 “(3) ACCESS TO INFORMATION.—The head of
25 an agency shall ensure that, to the greatest extent

1 practicable, information is included in the unclassi-
2 fied form of the report submitted by the agency
3 under paragraph (2)(A).

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

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

16 (4) in section 3555—

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

20 (B) in subsection (a)—

21 (i) in paragraph (1), by inserting
22 “during which a report is required to be
23 submitted under section 3553(c),” after
24 “Each year”;

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

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

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

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

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

16 (E) by striking subsection (f) and inserting
17 the following:

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

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

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

9 “(A) specific information system incidents; or

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

12 (F) in subsection (g)(2)—

13 (i) by striking “this subsection shall”

14 and inserting “this subsection—

15 “(A) shall”;

16 (ii) in subparagraph (A), as so des-

17 ignated, by striking the period at the end

18 and inserting “; and”; and

19 (iii) by adding at the end the fol-

20 lowing:

21 “(B) identify any entity that performs an

22 independent evaluation under subsection (b).”;

23 and

24 (G) striking subsection (j); and

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

3 (d) CONFORMING AMENDMENTS.—

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

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

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

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

“3555. Independent evaluation.”.

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

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

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

22 (i) by striking “annually thereafter”
23 and inserting “thereafter during the years

1 during which a report is required to be
2 submitted under section 3553(c) of title
3 44, United States Code”; and

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

7 (3) NIST RESPONSIBILITIES.—Section
8 20(d)(3)(B) of the National Institute of Standards
9 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is
10 amended by striking “annual”.

11 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

15 “SUBCHAPTER IV—FEDERAL SYSTEM
16 INCIDENT RESPONSE

17 “§ 3591. Definitions

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

21 “(b) ADDITIONAL DEFINITIONS.—As used in this
22 subchapter:

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

1 “(A) the majority and minority leaders of
2 the Senate;

3 “(B) the Speaker and minority leader of
4 the House of Representatives;

5 “(C) the Committee on Homeland Security
6 and Governmental Affairs of the Senate;

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

9 “(E) the Committee on Homeland Security
10 of the House of Representatives;

11 “(F) the appropriate authorization and ap-
12 propriations committees of Congress;

13 “(G) the Director;

14 “(H) the Director of the Cybersecurity and
15 Infrastructure Security Agency;

16 “(I) the National Cyber Director;

17 “(J) the Comptroller General of the United
18 States; and

19 “(K) the inspector general of any impacted
20 agency.

21 “(2) AWARDEE.—The term ‘awardee’—

22 “(A) means a person, business, or other
23 entity that receives a grant from, or is a party
24 to a cooperative agreement or an other trans-
25 action agreement with, an agency; and

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

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

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

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

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

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

23 “(8) NATIONWIDE CONSUMER REPORTING
24 AGENCY.—The term ‘nationwide consumer reporting
25 agency’ means a consumer reporting agency de-

1 scribed in section 603(p) of the Fair Credit Report-
2 ing Act (15 U.S.C. 1681a(p)).

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

6 **“§ 3592. Notification of breach**

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

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

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

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

23 “(C) the type of breach; and

24 “(D) any other factors determined by the
25 Director; and

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

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

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

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

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

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

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

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

22 “(B) may include a telephone number,
23 mailing address, or a website;

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

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

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

10 “(c) DELAY OF NOTIFICATION.—

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

15 “(A) impede a criminal investigation or a
16 national security activity;

17 “(B) reveal sensitive sources and methods;

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

19 “(D) hamper security remediation actions.

20 “(2) DOCUMENTATION.—

21 “(A) IN GENERAL.—Any delay under para-
22 graph (1) shall be reported in writing to the Di-
23 rector, the Attorney General, the Director of
24 National Intelligence, the Secretary of Home-
25 land Security, the National Cyber Director, the

1 Director of the Cybersecurity and Infrastruc-
2 ture Security Agency, and the head of the agen-
3 cy and the inspector general of the agency that
4 experienced the breach.

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

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

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

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

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

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

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

12 **“§ 3593. Congressional and executive branch reports**

13 “(a) INITIAL REPORT.—

14 “(1) IN GENERAL.—Not later than 72 hours
15 after an agency has a reasonable basis to conclude
16 that a major incident occurred, the head of the
17 agency impacted by the major incident shall submit
18 to the appropriate reporting entities a written re-
19 port. Within 7 days of a major incident determina-
20 tion, the head of the agency impacted shall coordi-
21 nate with the National Cyber Director, or their des-
22 ignee, to provide a briefing, along with any other
23 Federal entity determined appropriate by the Na-
24 tional Cyber Director, to the Committee on Home-
25 land Security and Governmental Affairs of the Sen-

1 ate, the Committee on Oversight and Reform of the
2 House of Representatives, the Committee on Home-
3 land Security of the House of Representatives, and
4 the appropriate authorization and appropriations
5 committees of Congress, in the manner requested by
6 the Congressional entities, taking into account—

7 “(A) the information known at the time of
8 the report, including the threat having likely
9 caused the major incident;

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

12 “(C) the classification level of the informa-
13 tion contained in the report.

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

20 “(A) a summary of the information avail-
21 able about the major incident, including how
22 the major incident occurred and, if applicable,
23 information relating to the major incident as a
24 breach, based on information available to agen-

1 cy officials as of the date on which the agency
2 submits the report;

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

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

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

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

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

24 “(B) may include a classified component.

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

9 “(1) vulnerabilities, means by which the major
10 incident occurred, and impacts to the agency relat-
11 ing to the major incident;

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

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

20 “(4) an assessment of the risk of harm to indi-
21 viduals potentially affected by the major incident
22 based on information available to agency officials as
23 of the date on which the agency provides the update;

24 “(5) an update to the assessment of the risk to
25 agency operations, or to impacts on other agency or

1 non-Federal entity operations, affected by the major
2 incident based on information available to agency of-
3 ficials as of the date on which the agency provides
4 the update; and

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

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

20 “(d) BIENNIAL REPORT.—Each agency shall submit
21 as part of the biannual report required under section
22 3554(c)(1) of this title a description of each major inci-
23 dent that occurred during the 2-year period preceding the
24 date on which the biannual report is submitted.

25 “(e) DELAY REPORT.—

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

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

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

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

19 “(2) maintain a historical archive and major in-
20 cident log of all reports and briefings provided under
21 the requirements of this section, which shall include
22 at a minimum an archive of the full contents of any
23 written report and associated documentation, the re-
24 porting agency, the date of submission, and a list of
25 the recipient Congressional entities, which shall be

1 made available upon request to the Congressional
2 entities listed under subsection (a)(1) and may, to
3 the extent practicable, utilize an internet accessible
4 portal for appropriate Congressional staff to directly
5 access the log and archived materials required to be
6 maintained under this paragraph.

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

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

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

14 “(2) Congress from requesting additional infor-
15 mation from agencies through reports, briefings, or
16 other means.

17 **“§ 3594. Government information sharing and inci-**
18 **dent response**

19 “(a) IN GENERAL.—

20 “(1) INCIDENT REPORTING.—Subject to limita-
21 tions in subsection (b), the head of each agency shall
22 provide the information described in paragraph (2)
23 relating to an incident affecting the agency, whether
24 the information is obtained by the Federal Govern-
25 ment directly or indirectly, to the Cybersecurity and

1 Infrastructure Security Agency, the Office of Man-
2 agement and Budget, and the Office of the National
3 Cyber Director in a manner specified by the Director
4 under subsection (b).

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

8 “(A) include detailed information about
9 the safeguards that were in place when the inci-
10 dent occurred;

11 “(B) whether the agency implemented the
12 safeguards described in subparagraph (A) cor-
13 rectly;

14 “(C) in order to protect against a similar
15 incident, identify—

16 “(i) how the safeguards described in
17 subparagraph (A) should be implemented
18 differently; and

19 “(ii) additional necessary safeguards;
20 and

21 “(D) include information to aid in incident
22 response, such as—

23 “(i) a description of the affected sys-
24 tems or networks;

1 “(ii) the estimated dates of when the
2 incident occurred; and

3 “(iii) information that could reason-
4 ably help identify the party that conducted
5 the incident, as appropriate.

6 “(3) INFORMATION SHARING.—To the greatest
7 extent practicable, the Director of the Cybersecurity
8 and Infrastructure Security Agency shall—

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

16 “(B) coordinate, in consultation with the
17 National Cyber Director, any necessary infor-
18 mation sharing efforts related to a major inci-
19 dent with the private sector.

20 “(4) NATIONAL SECURITY SYSTEMS.—Each
21 agency operating or exercising control of a national
22 security system shall share information about inci-
23 dents that occur on national security systems with
24 the Director of the Cybersecurity and Infrastructure
25 Security Agency to the extent consistent with stand-

1 ards and guidelines for national security systems
2 issued in accordance with law and as directed by the
3 President.

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

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

1 **“§ 3595. Responsibilities of contractors and awardees**

2 “(a) REPORTING.—

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

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

18 “(B) an incident or breach has occurred
19 with respect to a Federal information system
20 used or operated by the contractor or awardee
21 in connection with the contract, grant, coopera-
22 tive agreement, or other transaction agreement
23 of the contractor or awardee;

24 “(C) a component of any Federal informa-
25 tion system, or a system able to access, store,
26 or process Federal information, contains a secu-

1 rity vulnerability, including a supply chain com-
2 promise or an identified software or hardware
3 vulnerability; or

4 “(D) the contractor or awardee has re-
5 ceived information from the agency that the
6 contractor or awardee is not authorized to re-
7 ceive in connection with the contract, grant, co-
8 operative agreement, or other transaction agree-
9 ment of the contractor or awardee.

10 “(2) PROCEDURES.—

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

18 “(B) INCIDENT.—Following a report of an
19 incident by a contractor or awardee under para-
20 graph (1), an agency, in consultation with the
21 contractor or awardee, shall carry out the re-
22 quirements under section 3594 with respect to
23 the incident.

24 “(b) EFFECTIVE DATE.—This section shall apply on
25 and after the date that is 1 year after the date of the

1 enactment of the Federal Information Security Mod-
2 ernization Act of 2022 and shall apply with respect to any
3 contract entered into on or after such effective date.

4 **“§ 3596. Training**

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

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

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

16 “(2) the obligation of a covered individual to re-
17 port to the agency a confirmed major incident and
18 any suspected incident involving information in any
19 medium or form, including paper, oral, and elec-
20 tronic.

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

1 **“§ 3597. Analysis and report on Federal incidents**

2 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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

11 “(i) attacker tactics, techniques, and
12 procedures; and

13 “(ii) system vulnerabilities, including
14 previously unknown zero day exploitations,
15 unpatched systems, and information sys-
16 tem misconfigurations;

17 “(B) the scope and scale of incidents at
18 agencies;

19 “(C) common root causes of incidents
20 across multiple agencies;

21 “(D) agency incident response, recovery,
22 and remediation actions and the effectiveness of
23 those actions, as applicable;

24 “(E) lessons learned and recommendations
25 in responding to, recovering from, remediating,
26 and mitigating future incidents; and

1 “(F) trends across multiple Federal agen-
2 cies to address intrusion detection and incident
3 response capabilities using the metrics estab-
4 lished under section 224(c) of the Cybersecurity
5 Act of 2015 (6 U.S.C. 1522(c)).

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

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

11 “(A) IN GENERAL.—The Director shall
12 share on an ongoing basis the analyses required
13 under this subsection with agencies and the Na-
14 tional Cyber Director to—

15 “(i) improve the understanding of cy-
16 bersecurity risk of agencies; and

17 “(ii) support the cybersecurity im-
18 provement efforts of agencies.

19 “(B) FORMAT.—In carrying out subpara-
20 graph (A), the Director shall share the anal-
21 yses—

22 “(i) in human-readable written prod-
23 ucts; and

24 “(ii) to the greatest extent practicable,
25 in machine-readable formats in order to

1 enable automated intake and use by agen-
2 cies.

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

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

14 “(2) the quantitative and qualitative analyses of
15 incidents developed under subsection (a)(1) on an
16 agency-by-agency basis and comprehensively across
17 the Federal Government, including—

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

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

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

24 “(A) a description of each major incident;
25 and

1 “(B) an analysis of the agency’s perform-
2 ance against the metrics established under sec-
3 tion 224(c) of the Cybersecurity Act of 2015 (6
4 U.S.C. 1522(c)).

5 “(c) PUBLICATION.—To the extent that publication
6 is consistent with national security interests, a version of
7 each report submitted under subsection (b) shall be made
8 publicly available on the website of the Cybersecurity and
9 Infrastructure Security Agency during the year in which
10 the report is submitted.

11 “(d) INFORMATION PROVIDED BY AGENCIES.—

12 “(1) IN GENERAL.—The analysis required
13 under subsection (a) and each report submitted
14 under subsection (b) shall use information provided
15 by agencies under section 3594(a).

16 “(2) NATIONAL SECURITY SYSTEM REPORTS.—

17 “(A) IN GENERAL.—Annually, the head of
18 an agency that operates or exercises control of
19 a national security system shall submit a report
20 that includes the information described in sub-
21 section (b) with respect to the agency to the ex-
22 tent that the submission is consistent with
23 standards and guidelines for national security
24 systems issued in accordance with law and as
25 directed by the President to—

1 “(i) the majority and minority leaders
2 of the Senate,

3 “(ii) the Speaker and minority leader
4 of the House of Representatives;

5 “(iii) the Committee on Homeland Se-
6 curity and Governmental Affairs of the
7 Senate;

8 “(iv) the Select Committee on Intel-
9 ligence of the Senate;

10 “(v) the Committee on Armed Serv-
11 ices of the Senate;

12 “(vi) the Committee on Appropria-
13 tions of the Senate;

14 “(vii) the Committee on Oversight and
15 Reform of the House of Representatives;

16 “(viii) the Committee on Homeland
17 Security of the House of Representatives;

18 “(ix) the Permanent Select Committee
19 on Intelligence of the House of Represent-
20 atives;

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

23 “(xi) the Committee on Appropria-
24 tions of the House of Representatives.

1 “(B) CLASSIFIED FORM.—A report re-
2 quired under subparagraph (A) may be sub-
3 mitted in a classified form.

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

13 **“§ 3598. Major incident definition**

14 “(a) IN GENERAL.—Not later than 180 days after
15 the date of the enactment of the Federal Information Se-
16 curity Modernization Act of 2022, the Director, in coordi-
17 nation with the Director of the Cybersecurity and Infra-
18 structure Security Agency and the National Cyber Direc-
19 tor, shall develop and promulgate guidance on the defini-
20 tion of the term ‘major incident’ for the purposes of sub-
21 chapter II and this subchapter.

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

1 “(1) include, with respect to any information
2 collected or maintained by or on behalf of an agency
3 or an information system used or operated by an
4 agency or by a contractor of an agency or another
5 organization on behalf of an agency, any incident
6 the head of the agency determines is likely to result
7 in demonstrable harm to—

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

10 “(B) the public confidence, civil liberties,
11 or public health and safety of the people of the
12 United States;

13 “(C) the integrity of personally identifiable
14 information, including the exfiltration, modifica-
15 tion, or deletion of such information; or

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

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

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

23 “(B) is enabled by—

24 “(i) a common technical root cause,
25 such as a supply chain compromise or a

1 common software or hardware vulner-
2 ability; or

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

5 “(C) has a significant impact on the con-
6 fidentiality, integrity, or availability of a high
7 value asset.

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

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

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

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

23 (2) CLERICAL AMENDMENT.—The table of sec-
24 tions for chapter 35 of title 44, United States Code,
25 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.”.

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

2 (a) MODERNIZING GOVERNMENT TECHNOLOGY.—

3 Subtitle G of title X of Division A of the National Defense
4 Authorization Act for Fiscal Year 2018 (Public Law 115–
5 91; 40 U.S.C. 11301 note) is amended in section 1078—

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

8 “(a) DEFINITIONS.—In this section:

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

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

15 (2) in subsection (c)—

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

19 (B) in paragraph (5)—

20 (i) in subparagraph (A), by striking

21 “and” at the end;

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

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

6 “(C) a senior official from the Cybersecu-
7 rity and Infrastructure Security Agency of the
8 Department of Homeland Security, appointed
9 by the Director.”; and

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

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

15 (1) in section 11302—

16 (A) in subsection (b), by striking “use, se-
17 curity, and disposal of” and inserting “use, and
18 disposal of, and, in consultation with the Direc-
19 tor of the Cybersecurity and Infrastructure Se-
20 curity Agency and the National Cyber Director,
21 promote and improve the security of,”;

22 (B) in subsection (c)(3)(B), by adding at
23 the end the following:

24 “(iii) The Director may make avail-
25 able, upon request, to the National Cyber

1 Director any cybersecurity funding infor-
2 mation provided to the Director under
3 clause (ii) of this subparagraph.”;

4 (C) in subsection (f), by striking “The Di-
5 rector shall” and inserting “The Director
6 shall—

7 “(1) encourage the heads of the executive agen-
8 cies to develop and use the best practices in the ac-
9 quisition of information technology, including supply
10 chain risk management standards, guidelines, and
11 practices developed by the National Institute of
12 Standards and Technology; and

13 “(2) consult with the Federal Chief Information
14 Security Officer appointed by the President under
15 section 3607 of title 44, for the development and use
16 of risk management standards, guidelines, and prac-
17 tices developed by the National Institute of Stand-
18 ards and Technology.”; and

19 (D) in subsection (h), by inserting “, in-
20 cluding cybersecurity performances,” after “the
21 performances”; and

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

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

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

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

4 “(iii) whether the function should be
5 performed by a shared service offered by
6 another executive agency.”.

7 (c) SUBCHAPTER II.—Subchapter II of chapter 113
8 of subtitle III of title 40, United States Code, is amend-
9 ed—

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

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

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

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

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

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

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

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

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

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

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

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

15 “(e) REVIEW OF OFFICE OF MANAGEMENT AND
16 BUDGET GUIDANCE AND POLICY.—

17 “(1) CONDUCT OF REVIEW.—

18 “(A) IN GENERAL.—Not less frequently
19 than once every 3 years, the Director of the Of-
20 fice of Management and Budget, in consultation
21 with, as available, the Chief Information Offi-
22 cers Council, the Director of the Cybersecurity
23 and Infrastructure Security Agency, the Na-
24 tional Cyber Director, the Comptroller General
25 of the United States, and the Council of the In-

1 spectors General on Integrity and Efficiency,
2 shall review the efficacy of the guidance and
3 policy promulgated by the Director in reducing
4 cybersecurity risks, including an assessment of
5 the requirements for agencies to report infor-
6 mation to the Director, and determine whether
7 any changes to that guidance or policy is appro-
8 priate.

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

14 “(C) REQUIREMENTS BURDEN REDUCTION
15 AND CLARITY.—In conducting the review de-
16 scribed in subparagraph (A), the Director shall
17 consider the cumulative reporting and compli-
18 ance burden to agencies as well as the clarity
19 of the requirements and deadlines contained in
20 guidance and policy documents.

21 “(2) UPDATED GUIDANCE.—Not later than 90
22 days after the date on which a review is completed
23 under paragraph (1), the Director of the Office of
24 Management and Budget shall issue updated guid-

1 ance or policy to agencies determined appropriate by
2 the Director, based on the results of the review.

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

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

15 “(B) the cybersecurity risk mitigation, or
16 other cybersecurity benefit, offered by each
17 guidance or policy document described in sub-
18 paragraph (A); and

19 “(C) a summary of the guidance or policy
20 to which changes were determined appropriate
21 during the review and what the changes in-
22 clude.

23 “(f) AUTOMATED STANDARD IMPLEMENTATION
24 VERIFICATION.—When the Director of the National Insti-
25 tute of Standards and Technology issues a proposed

1 standard pursuant to paragraphs (2) and (3) of section
2 20(a) of the National Institute of Standards and Tech-
3 nology Act (15 U.S.C. 278g-3(a)), the Director of the Na-
4 tional Institute of Standards and Technology shall con-
5 sider developing and, if appropriate and practical, develop,
6 in consultation with the Director of the Cybersecurity and
7 Infrastructure Security Agency, specifications to enable
8 the automated verification of the implementation of con-
9 trols.”.

10 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**
11 **SPONSE.**

12 (a) RESPONSIBILITIES OF THE CYBERSECURITY AND
13 INFRASTRUCTURE SECURITY AGENCY.—

14 (1) IN GENERAL.—Not later than 180 days
15 after the date of the enactment of this Act, the Di-
16 rector of the Cybersecurity and Infrastructure Secu-
17 rity Agency shall—

18 (A) develop a plan for the development of
19 the analysis required under section 3597(a) of
20 title 44, United States Code, as added by this
21 Act, and the report required under subsection
22 (b) of that section that includes—

23 (i) a description of any challenges the
24 Director anticipates encountering; and

1 (ii) the use of automation and ma-
2 chine-readable formats for collecting, com-
3 piling, monitoring, and analyzing data; and

4 (B) provide to the appropriate congres-
5 sional committees a briefing on the plan devel-
6 oped under subparagraph (A).

7 (2) BRIEFING.—Not later than 1 year after the
8 date of the enactment of this Act, the Director of
9 the Cybersecurity and Infrastructure Security Agen-
10 cy shall provide to the appropriate congressional
11 committees a briefing on—

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

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

17 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
18 OFFICE OF MANAGEMENT AND BUDGET.—

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

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

23 (B) by redesignating subsections (c)
24 through (f) as subsections (b) through (e), re-
25 spectively.

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

7 (3) GUIDANCE ON RESPONDING TO INFORMA-
8 TION REQUESTS.—Not later than 1 year after the
9 date of the enactment of this Act, the Director shall
10 develop guidance for agencies to implement the re-
11 quirement under section 3594(c) of title 44, United
12 States Code, as added by this Act, to provide infor-
13 mation to other agencies experiencing incidents.

14 (4) STANDARD GUIDANCE AND TEMPLATES.—
15 Not later than 1 year after the date of the enact-
16 ment of this Act, the Director, in consultation with
17 the Director of the Cybersecurity and Infrastructure
18 Security Agency, shall develop guidance and tem-
19 plates, to be reviewed and, if necessary, updated not
20 less frequently than once every 2 years, for use by
21 Federal agencies in the activities required under sec-
22 tions 3592, 3593, and 3596 of title 44, United
23 States Code, as added by this Act.

24 (5) CONTRACTOR AND AWARDEE GUIDANCE.—

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

14 (B) EXISTING PROCESSES.—To the great-
15 est extent practicable, the guidance issued
16 under subparagraph (A) shall allow contractors
17 and awardees to use existing processes for noti-
18 fying Federal agencies of incidents involving in-
19 formation of the Federal Government.

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

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

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

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

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

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

17 **SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**
18 **UPDATES.**

19 Not later than 1 year after the date of the enactment
20 of this Act, the Director shall issue guidance for agencies
21 on—

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

1 (2) implementing additional cybersecurity pro-
2 cedures, which shall include resources for shared
3 services;

4 (3) establishing a process for providing the sta-
5 tus of each remedial action under section 3554(b)(7)
6 of title 44, United States Code, as amended by this
7 Act, to the Director and the Director of the Cyberse-
8 curity and Infrastructure Security Agency using au-
9 tomation and machine-readable data, as practicable,
10 which shall include—

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

13 (B) templates for providing the status of
14 the remedial action;

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

18 (5) a requirement to coordinate with inspectors
19 general of agencies to ensure consistent under-
20 standing and application of agency policies for the
21 purpose of evaluations by inspectors general.

22 **SEC. 105. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**
23 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

24 (a) **DEFINITIONS.**—In this section:

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

5 (2) SENSITIVE INFORMATION.—The term “sen-
6 sitive information” has the meaning given the term
7 by the Director in guidance issued under subsection
8 (b).

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

14 (1) the confidentiality or integrity of sensitive
15 information submitted by the reporting entity to the
16 agency pursuant to a statutory or regulatory re-
17 quirement; or

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

21 **TITLE II—IMPROVING FEDERAL** 22 **CYBERSECURITY**

23 **SEC. 201. MOBILE SECURITY STANDARDS.**

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

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

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

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

7 (1) a requirement, pursuant to section
8 3506(b)(4) of title 44, United States Code, for every
9 agency to maintain a continuous inventory of
10 every—

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

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

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

19 (c) INFORMATION SHARING.—The Director, in co-
20 ordination with the Director of the Cybersecurity and In-
21 frastructure Security Agency, shall issue guidance to
22 agencies for sharing the inventory of the agency required
23 under subsection (b)(1) with the Director of the Cyberse-
24 curity and Infrastructure Security Agency, using automa-

1 tion and machine-readable data to the greatest extent
2 practicable.

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

9 **SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT**
10 **RESPONSE.**

11 (a) RECOMMENDATIONS.—Not later than 2 years
12 after the date of the enactment of this Act, and not less
13 frequently than every 2 years thereafter, the Director of
14 the Cybersecurity and Infrastructure Security Agency, in
15 consultation with the Attorney General, shall submit to
16 the Director recommendations on requirements for logging
17 events on agency systems and retaining other relevant
18 data within the systems and networks of an agency.

19 (b) CONTENTS.—The recommendations provided
20 under subsection (a) shall include—

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

22 (2) the duration that logs and other relevant
23 data should be retained;

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

1 (4) how to ensure the confidentiality, integrity,
2 and availability of logs;

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

9 (A) the Director of the Cybersecurity and
10 Infrastructure Security Agency for a cybersecu-
11 rity purpose; and

12 (B) the Director of the Federal Bureau of
13 Investigation, or the appropriate Federal law
14 enforcement agency, to investigate potential
15 criminal activity; and

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

21 (c) GUIDANCE.—Not later than 90 days after receiv-
22 ing the recommendations submitted under subsection (a),
23 the Director, in consultation with the Director of the Cy-
24 bersecurity and Infrastructure Security Agency and the
25 Attorney General, shall, as determined to be appropriate

1 by the Director, update guidance to agencies regarding re-
2 quirements for logging, log retention, log management,
3 sharing of log data with other appropriate agencies, or any
4 other logging activity determined to be appropriate by the
5 Director.

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

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

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

13 **“§ 3559A. Federal penetration testing**

14 “(a) GUIDANCE.—

15 “(1) IN GENERAL.—The Director shall, in con-
16 sultation with the Secretary of the Department of
17 Homeland Security acting through the Director of
18 the Cybersecurity and Infrastructure Security Agen-
19 cy, issue guidance to agencies that—

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

24 “(B) provides policies governing agency de-
25 velopment of an operational plan, rules of en-

1 gagement for utilizing penetration testing, and
2 procedures to utilize the results of penetration
3 testing to improve the cybersecurity and risk
4 management of the agency; and

5 “(C) establishes a program under the Cy-
6 bersecurity and Infrastructure Security Agency
7 to ensure that penetration testing is being per-
8 formed appropriately by agencies and to provide
9 operational support or a shared service.

10 “(b) RESPONSIBILITIES OF OMB.—The Director, in
11 coordination with the Director of the Cybersecurity and
12 Infrastructure Security Agency, shall—

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

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

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

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

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

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

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

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

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

 “3559A. Federal penetration testing.”.

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

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

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

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

1 “(9) performing penetration testing to identify
2 vulnerabilities within Federal information systems;
3 and”.

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

5 (a) **THREAT HUNTING PROGRAM.**—

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

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

22 (A) determine the method for collecting,
23 storing, accessing, analyzing, and safeguarding
24 appropriate agency data;

1 (B) provide on-premises support to agen-
2 cies;

3 (C) staff threat hunting services;

4 (D) allocate available human and financial
5 resources to implement the plan; and

6 (E) provide input to the heads of agencies
7 on the use of—

8 (i) more stringent standards under
9 section 11331(c)(1) of title 40, United
10 States Code; and

11 (ii) additional cybersecurity proce-
12 dures under section 3554 of title 44,
13 United States Code.

14 (b) REPORTS.—The Director of the Cybersecurity
15 and Infrastructure Security Agency, in consultation with
16 the Director, shall submit to the appropriate congressional
17 committees—

18 (1) not later than 30 days after the date on
19 which the Director of the Cybersecurity and Infra-
20 structure Security Agency completes the plan re-
21 quired under subsection (a)(2), a report on the plan
22 to provide threat hunting services to agencies;

23 (2) not less than 30 days before the date on
24 which the Director of the Cybersecurity and Infra-
25 structure Security Agency begins providing threat

1 hunting services under the program under sub-
2 section (a)(1), a report providing any updates to the
3 plan developed under subsection (a)(2); and
4 (3) not later than 1 year after the date on
5 which the Director of the Cybersecurity and Infra-
6 structure Security Agency begins providing threat
7 hunting services to agencies other than the Cyberse-
8 curity and Infrastructure Security Agency, a report
9 describing lessons learned from providing those serv-
10 ices.

11 **SEC. 205. CODIFYING VULNERABILITY DISCLOSURE PRO-**
12 **GRAMS.**

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

16 **“§ 3559B. Federal vulnerability disclosure programs**

17 “(a) DEFINITIONS.—In this section:

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

21 “(2) REPORTER.—The term ‘reporter’ means
22 an individual that submits a vulnerability report
23 pursuant to the vulnerability disclosure process of an
24 agency.

25 “(b) RESPONSIBILITIES OF OMB.—

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

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

11 “(B) is authorized under the vulnerability
12 disclosure policy of the agency developed under
13 subsection (d)(2).

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

23 “(A) any valid or credible reports of newly
24 discovered or not publicly known vulnerabilities
25 (including misconfigurations) on Federal infor-

1 mation systems that use commercial software or
2 services;

3 “(B) information relating to vulnerability
4 disclosure, coordination, or remediation activi-
5 ties of an agency, particularly as those activities
6 relate to outside organizations—

7 “(i) with which the head of the agency
8 believes the Director of the Cybersecurity
9 and Infrastructure Security Agency can as-
10 sist; or

11 “(ii) about which the head of the
12 agency believes the Director of the Cyber-
13 security and Infrastructure Security Agen-
14 cy should know; and

15 “(C) any other information with respect to
16 which the head of the agency determines helpful
17 or necessary to involve the Director of the Cy-
18 bersecurity and Infrastructure Security Agency.

19 “(3) AGENCY VULNERABILITY DISCLOSURE
20 POLICIES.—The Director shall issue guidance to
21 agencies on the required minimum scope of agency
22 systems covered by the vulnerability disclosure policy
23 of an agency required under subsection (d)(2).

1 “(c) RESPONSIBILITIES OF CISA.—The Director of
2 the Cybersecurity and Infrastructure Security Agency
3 shall—

4 “(1) provide support to agencies with respect to
5 the implementation of the requirements of this sec-
6 tion;

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

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

14 “(d) RESPONSIBILITIES OF AGENCIES.—

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

19 “(A) an appropriate security contact; and

20 “(B) the component of the agency that is
21 responsible for the internet accessible services
22 offered at the domain.

23 “(2) VULNERABILITY DISCLOSURE POLICY.—

24 The head of each agency shall develop and make

1 publicly available a vulnerability disclosure policy for
2 the agency, which shall—

3 “(A) describe—

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

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

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

12 “(iv) the disclosure policy of the agen-
13 cy for sensitive information;

14 “(B) with respect to a report to an agency,
15 describe—

16 “(i) how the reporter should submit
17 the report; and

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

22 “(C) include any other relevant informa-
23 tion; and

24 “(D) be mature in scope, covering all inter-
25 net accessible Federal information systems used

1 or operated by that agency or on behalf of that
2 agency.

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

8 “(e) CONGRESSIONAL REPORTING.—Not later than
9 90 days after the date of the enactment of the Federal
10 Information Security Modernization Act of 2022, and an-
11 nually thereafter for a 3-year period, the Director of the
12 Cybersecurity and Infrastructure Security Agency, in con-
13 sultation with the Director, shall provide to the Committee
14 on Homeland Security and Governmental Affairs of the
15 Senate and the Committee on Oversight and Reform of
16 the House of Representatives a briefing on the status of
17 the use of vulnerability disclosure policies under this sec-
18 tion at agencies, including, with respect to the guidance
19 issued under subsection (b)(3), an identification of the
20 agencies that are compliant and not compliant.

21 “(f) EXEMPTIONS.—The authorities and functions of
22 the Director and Director of the Cybersecurity and Infra-
23 structure Security Agency under this section shall not
24 apply to national security systems.

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

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

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

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

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

 “3559B. Federal vulnerability disclosure programs”.

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

18 (a) GUIDANCE.—The Director shall maintain guid-
19 ance on the adoption of zero trust architecture and not
20 later than 2 years after the date of the enactment of this
21 Act, provide an update to the appropriate congressional
22 committees on progress in increasing the internal defenses
23 of agency systems through such adoption across the gov-
24 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 as quickly as practicable, ac-
12 counting for intelligence or law enforcement pur-
13 poses;

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

16 (7) a summary of the agency progress reports
17 required under subsection (b).

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

24 (1) a description of any steps the agency has
25 completed, including progress toward achieving any

1 requirements issued by the Director, including the
2 adoption of any models or reference architecture;

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

6 (3) a schedule to implement any planned activi-
7 ties.

8 **SEC. 207. GAO AUTOMATION REPORT.**

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

17 **SEC. 208. EXTENSION OF FEDERAL ACQUISITION SECURITY**
18 **COUNCIL.**

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

22 (b) DESIGNATION.—Section 1322(c)(1) of title 41,
23 United States Code, is amended by striking “Not later
24 than” and all that follows through the end of the para-
25 graph and inserting the following: “The Director of OMB

1 shall designate the Federal Chief Information Security Of-
2 ficer appointed by the President under section 3607 of
3 title 44, or an equivalent senior-level official from the Of-
4 fice of Management and Budget if the position is vacant,
5 to serve as the Chairperson of the Council.”.

6 (c) REQUIREMENT.—Subsection 1326(b) of title 41,
7 United States Code, is amended—

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

10 (2) by redesignating paragraph (6) as para-
11 graph (7); and

12 (3) by inserting after paragraph (5) the fol-
13 lowing new paragraph:

14 “(6) maintaining an up-to-date and accurate in-
15 ventory of software in use by the agency and, when
16 available, the components of such software, including
17 any available Software Bills of Materials, as applica-
18 ble, that can be communicated when requested to
19 the Federal Acquisition Security Council, the Na-
20 tional Cybersecurity Director, or the Secretary of
21 Homeland Security acting through the Director of
22 Cybersecurity and Infrastructure Security Agency.”.

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

3 (a) AMENDMENT.—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;

20 “(4) assisting the Director with carrying out
21 budget formation duties under subtitle II of title 31
22 as it pertains to the information technology, oper-
23 ations, and workforce resources of Federal agencies
24 to fulfill cybersecurity responsibilities under section
25 3554, and the duties of the Department of Home-

1 land Security duties designated under section 3553;
2 and

3 “(5) other initiatives determined by the Chief
4 Information Officer.

5 “(c) ADDITIONAL DUTIES.—The Federal Chief Infor-
6 mation Security Officer shall work with the Chief Informa-
7 tion Officer to oversee implementation of electronic Gov-
8 ernment under the E–Government Act of 2002, and other
9 relevant statutes, in a manner consistent with law, relating
10 to—

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

14 “(2) the development of enterprise architec-
15 tures;

16 “(3) information security;

17 “(4) privacy;

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

20 “(6) other areas of electronic Government as
21 determined by the Administrator.

22 “(d) ASSISTANCE.—The Federal Chief Information
23 Security Officer shall assist the Administrator in the per-
24 formance of electronic Government functions as described
25 in section 3602(f).”.

1 (b) DEPUTY NATIONAL CYBER DIRECTOR.—Section
2 1752 of the William M. (Mac) Thornberry National De-
3 fense Authorization Act for Fiscal Year 2021 (6 U.S.C.
4 1500; 134 Stat. 4144) is amended by adding at the end
5 the following new subsection:

6 “(d) DEPUTY DIRECTOR.—There shall be a Deputy
7 National Cyber Director for Agency Strategy, Capabilities,
8 and Budget, who shall be the Federal Chief Information
9 Security Officer appointed by the President under section
10 3607 of title 44, United States Code, and shall report to
11 the Director and assist the office in carrying out the fol-
12 lowing duties as it applies to the protection of Federal in-
13 formation systems by the agencies—

14 “(1) the preparation and oversight over the im-
15 plementation of national cyber policy and strategy
16 under subsection (c)(1)(C)(i);

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

20 “(3) reviewing annual budget proposals and
21 making related recommendations under subsection
22 (c)(1)(C)(iii);

23 “(4) the functions, as determined necessary, of
24 the National Cyber Director under subchapter II of
25 chapter 35 of title 44, United States Code; and

1 identified in the independent evaluations re-
2 quired by section 3555(a) of title 44, United
3 States Code; and”.

4 **SEC. 212. QUANTITATIVE CYBERSECURITY METRICS.**

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

9 (b) UPDATING AND ESTABLISHING METRICS.—Not
10 later than 1 year after the date of the enactment of this
11 Act, the Director of the Cybersecurity and Infrastructure
12 Security Agency, in coordination with the Director and
13 consulting with the Director of the National Institute of
14 Standards and Technology, shall—

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

17 (2) as appropriate and pursuant to section
18 224(c) of the Cybersecurity Act of 2015 (6 U.S.C.
19 1522(c))—

20 (A) update the covered metrics; and

21 (B) establish new covered metrics.

22 (c) IMPLEMENTATION.—

23 (1) IN GENERAL.—Not later than 540 days
24 after the date of the enactment of this Act, the Di-
25 rector, in coordination with the Director of the Cy-

1 bersecurity and Infrastructure Security Agency,
2 shall promulgate guidance that requires each agency
3 to use covered metrics to track trends in the cyber-
4 security and incident response capabilities of the
5 agency.

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

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

22 (4) ANALYSIS CAPACITY.—The Director of the
23 Cybersecurity and Infrastructure Security Agency
24 shall develop a capability that allows for the analysis
25 of the covered metrics, including cross-agency per-

1 performance of agency cybersecurity and incident re-
2 sponse capability trends.

3 (d) CONGRESSIONAL REPORTS.—

4 (1) UTILITY OF METRICS.—Not later than 1
5 year after the date of the enactment of this Act, the
6 Director of the Cybersecurity and Infrastructure Se-
7 curity Agency, in coordination with the Director,
8 shall submit to the appropriate congressional com-
9 mittees a report on the utility of the covered metrics.

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

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

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

22 (2) in section 224—

23 (A) by amending subsection (c) to read as
24 follows:

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

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

9 (C) by redesignating subsection (f) as sub-
10 section (e).

11 **TITLE III—PILOT PROGRAMS TO**
12 **ENHANCE FEDERAL CYBER-**
13 **SECURITY**

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

15 (a) DEFINITIONS.—In this section:

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

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

22 (B) the Committee on Homeland Security,
23 the Committee on Oversight and Reform, and
24 the Committee on Appropriations of the House
25 of Representatives.

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

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

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

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

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

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

21 (b) ESTABLISHMENT OF RISK-BASED BUDGET
22 PILOT.—

23 (1) IN GENERAL.—

24 (A) MODEL.—Not later than 1 year after
25 the first publication of the budget submitted by

1 the President under section 1105 of title 31,
2 United States Code, following the date of the
3 enactment of this Act, the Director, in consulta-
4 tion with the Director of the Cybersecurity and
5 Infrastructure Security Agency and the Na-
6 tional Cyber Director and in coordination with
7 the Director of the National Institute of Stand-
8 ards and Technology, shall conduct a pilot for
9 creating a risk-based budget for cybersecurity
10 spending.

11 (B) CONTENTS OF PILOT.—The pilot re-
12 quired to be developed under this paragraph
13 shall—

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

18 (ii) consider the impact on agency op-
19 erations of incidents, including the
20 interconnectivity to other agency systems
21 and the operations of other agencies;

22 (iii) indicate where resources should
23 be allocated to have the greatest impact on
24 mitigating current and future threats and

1 current and future cybersecurity capabili-
2 ties;

3 (iv) be used to inform acquisition and
4 sustainment of—

5 (I) information technology and
6 cybersecurity tools;

7 (II) information technology and
8 cybersecurity architectures;

9 (III) information technology and
10 cybersecurity personnel; and

11 (IV) cybersecurity and informa-
12 tion technology concepts of operations;
13 and

14 (v) be used to evaluate and inform
15 government-wide cybersecurity programs of
16 the Department of Homeland Security.

17 (2) REPORTS.—Not later than 2 years after the
18 first publication of the budget submitted by the
19 President under section 1105 of title 31, United
20 States Code, following the date of the enactment of
21 this Act, the Director shall submit a report to Con-
22 gress on the implementation of the pilot for risk-
23 based budgeting for cybersecurity spending, an as-
24 sessment of agency implementation, and an evalua-

1 tion of whether the risk-based budget helps to miti-
2 gate cybersecurity vulnerabilities.

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

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

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

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

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

21 (a) DEFINITION.—In this section, the term “active
22 defense technique” has the meaning given in guidance
23 issued by the Director, in coordination with the Attorney
24 General.

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

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

11 (2) an evaluation of—

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

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

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

1 security activities, including intelligence collection;
2 and

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

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

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

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

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

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

23 (2) staffing and resources; and

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

1 (d) PILOT PROGRAM.—

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

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

17 (e) BRIEFING AND REPORT.—

18 (1) BRIEFING.—Not later than 270 days after
19 the date of the enactment of this Act, the Director
20 of the Cybersecurity and Infrastructure Security
21 Agency shall provide to appropriate congressional
22 committees a briefing on the parameters of any 1-
23 year agreements entered into under subsection
24 (d)(1).

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

7 (A) the agreement; and

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

10 **SEC. 304. ENDPOINT DETECTION AND RESPONSE AS A**
11 **SERVICE PILOT.**

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

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

1 (c) CONTENTS.—The plan required under subsection

2 (b) shall include considerations for—

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

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

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

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

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

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

21 (d) PILOT PROGRAM.—

22 (1) IN GENERAL.—Not later than 180 days
23 after the date on which the plan required under sub-
24 section (b) is developed, the Director of the Cyberse-
25 curity and Infrastructure Security Agency, in con-

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

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

11 (e) BRIEFING AND REPORT.—

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

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

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

6 (A) the agreement; and

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