

117TH CONGRESS
1ST SESSION

S. 2902

To modernize Federal information security management, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 29, 2021

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To modernize Federal information security management, 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 2021”.

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 entities impacted by incidents.

TITLE II—IMPROVING FEDERAL CYBERSECURITY

- Sec. 201. Evaluation of effectiveness of standards.
 Sec. 202. Mobile security standards.
 Sec. 203. Quantitative cybersecurity metrics.
 Sec. 204. Data and logging retention for incident response.
 Sec. 205. CISA agency advisors.
 Sec. 206. Federal penetration testing policy.
 Sec. 207. Ongoing threat hunting program.
 Sec. 208. Codifying vulnerability disclosure programs.
 Sec. 209. Implementing presumption of compromise and zero trust architectures.
 Sec. 210. Automation reports.
 Sec. 211. Extension of Federal Acquisition Security Council.

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

- Sec. 301. Continuous independent FISMA evaluation pilot.
 Sec. 302. Active cyber defensive pilot.
 Sec. 303. Security operations center as a service pilot.

1 **SEC. 3. DEFINITIONS.**

2 In this Act, unless otherwise specified:

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

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

11 (3) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—
 12
 13

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

3 (B) the Committee on Oversight and Re-
4 form of the House of Representatives; and

5 (C) the Committee on Homeland Security
6 of the House of Representatives.

7 (4) DIRECTOR.—The term “Director” means
8 the Director of the Office of Management and Budg-
9 et.

10 (5) INCIDENT.—The term “incident” has the
11 meaning given the term in section 3552(b) of title
12 44, United States Code.

13 (6) PENETRATION TEST.—The term “penetra-
14 tion test” has the meaning given the term in section
15 3552(b) of title 44, United States Code, as amended
16 by this Act.

17 (7) THREAT HUNTING.—The term “threat
18 hunting” means proactively and iteratively searching
19 for threats to systems that evade detection by auto-
20 mated threat detection systems.

21 (8) VERIFICATION SPECIFICATION.—The term
22 “verification specification” means a specification de-
23 veloped under section 11331(f) of title 40, United
24 States Code, as amended by this Act.

TITLE I—UPDATES TO FISMA

SEC. 101. TITLE 44 AMENDMENTS.

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

(1) in section 3504—

(A) in subsection (a)(1)(B)(v), by striking “confidentiality, security, disclosure, and sharing of information” and inserting “disclosure, sharing of information, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, confidentiality and security”;

(B) in subsection (b)(2)(B), by inserting “in coordination with the Director of the Cybersecurity and Infrastructure Security Agency” after “standards for security”;

(C) in subsection (g), by striking paragraph (1) and inserting the following:

“(1) with respect to information collected or maintained by or for agencies—

“(A) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, disclosure, and sharing of the information; and

1 “(B) in consultation with the Director of
2 the Cybersecurity and Infrastructure Security
3 Agency, develop and oversee policies, principles,
4 standards, and guidelines on confidentiality and
5 security of the information; and”;

6 (D) in subsection (h)(1)—

7 (i) in the matter preceding subpara-
8 graph (A)—

9 (I) by inserting “the Director of
10 the Cybersecurity and Infrastructure
11 Security Agency,” before “the Direc-
12 tor”;

13 (II) by inserting a comma before
14 “and the Administrator”;

15 (ii) in subparagraph (A), by inserting
16 “security and” after “information tech-
17 nology”;

18 (2) in section 3505—

19 (A) in paragraph (3) of the first subsection
20 designated as subsection (c)—

21 (i) in subparagraph (B)—

22 (I) by inserting “and the Direc-
23 tor of the Cybersecurity and Infra-
24 structure Security Agency” after
25 “Comptroller General”;

1 (II) by striking “and” at the end;

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

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

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

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

12 (3) in section 3506—

13 (A) in subsection (b)—

14 (i) in paragraph (1)(C), by inserting
15 “, availability” after “integrity”; and

16 (ii) in paragraph (4), by inserting
17 “the Director of the Cybersecurity and In-
18 frastructure Security Agency,” after “Gen-
19 eral Services,”; and

20 (B) in subsection (h)(3), by inserting “se-
21 curity,” after “efficiency,”;

22 (4) in section 3513—

23 (A) in subsection (a), by inserting “the Di-
24 rector of the Cybersecurity and Infrastructure

1 Security Agency,” before “the Administrator of
2 General Services”;

3 (B) by redesignating subsection (c) as sub-
4 section (d); and

5 (C) by inserting after subsection (b) the
6 following:

7 “(c) Each agency providing a written plan under sub-
8 section (b) shall provide any portion of the written plan
9 addressing information security or cybersecurity to the Di-
10 rector of the Cybersecurity and Infrastructure Security
11 Agency.”; and

12 (5) in section 3520A(b)—

13 (A) in paragraph (1), by striking “, protec-
14 tion”;

15 (B) by redesignating paragraphs (2), (3),
16 (4), and (5) as paragraphs (3), (4), (5), and
17 (6), respectively; and

18 (C) by inserting after paragraph (1) the
19 following:

20 “(2) in consultation with the Director of the
21 Cybersecurity and Infrastructure Security Agency,
22 establish Governmentwide best practices for the pro-
23 tection of data;”.

24 (b) SUCHAPTER II DEFINITIONS.—

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

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

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

8 “(1) The term ‘additional cybersecurity proce-
9 dure’ means a process, procedure, or other activity
10 that is established in excess of the information secu-
11 rity standards promulgated under section 11331(b)
12 of title 40 to increase the security and reduce the cy-
13 bersecurity risk of agency systems, such as contin-
14 uous threat hunting, increased network segmenta-
15 tion, endpoint detection and response, or persistent
16 penetration testing.”;

17 (C) by inserting after paragraph (6), as so
18 redesignated, the following:

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

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

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

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

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

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

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

19 “(12) The term ‘shared service’ means a busi-
20 ness or mission function that is provided for use by
21 multiple organizations within or between agencies.

22 “(13) The term ‘verification specification’
23 means a specification developed under section
24 11331(f) of title 40.”.

25 (2) CONFORMING AMENDMENTS.—

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

6 (B) TITLE 10.—

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

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

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

20 (iv) SECTION 2339A.—Section
21 2339a(e)(5) of title 10, United States
22 Code, is amended by striking “section
23 3552(b)(6)” and inserting “section
24 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) by redesignating paragraphs (3), (4),
12 (5), and (6) as paragraphs (4), (5), (6), and
13 (7), respectively;

14 (B) by inserting after paragraph (2) the
15 following:

16 “(3) recognize the role of the Cybersecurity and
17 Infrastructure Security Agency as the lead cyberse-
18 curity entity for operational coordination across the
19 Federal Government;”;

20 (C) in paragraph (5), as so redesignated,
21 by striking “diagnose and improve” and insert-
22 ing “integrate, deliver, diagnose, and improve”;

23 (D) in paragraph (6), as so redesignated,
24 by striking “and” at the end; and

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

1 “(8) recognize that each agency has specific
2 mission requirements and, at times, unique cyberse-
3 curity requirements to meet the mission of the agen-
4 cy;

5 “(9) recognize that each agency does not have
6 the same resources to secure agency systems, and an
7 agency should not be expected to have the capability
8 to secure the systems of the agency from advanced
9 adversaries alone; and

10 “(10) recognize that—

11 “(A) a holistic Federal cybersecurity model
12 is necessary to account for differences between
13 the missions and capabilities of agencies; and

14 “(B) in accounting for the differences de-
15 scribed in subparagraph (A) and ensuring over-
16 all Federal cybersecurity—

17 “(i) the Office of Management and
18 Budget is the leader for policy development
19 and oversight of Federal cybersecurity;

20 “(ii) the Cybersecurity and Infrastruc-
21 ture Security Agency is the leader for im-
22 plementing operations at agencies; and

23 “(iii) the National Cyber Director is
24 responsible for developing the overall cy-
25 bersecurity strategy of the United States

1 and advising the President on matters re-
2 lating to cybersecurity.”;

3 (2) in section 3553, as amended by section
4 1705 of the William M. (Mac) Thornberry National
5 Defense Authorization Act for Fiscal Year 2021
6 (Public Law 116–283)—

7 (A) in subsection (a)—

8 (i) in paragraph (1)—

9 (I) by striking “developing and”
10 and inserting “in coordination with
11 the Director of the Cybersecurity and
12 Infrastructure Security Agency,”; and

13 (II) by inserting “and associated
14 verification specifications” before
15 “promulgated”; and

16 (ii) in paragraph (5), by inserting “,
17 in coordination with the Director of the
18 Cybersecurity and Infrastructure Security
19 Agency,” before “agency compliance”;

20 (B) in subsection (b)—

21 (i) by striking the subsection heading
22 and inserting “CYBERSECURITY AND IN-
23 FRASTRUCTURE SECURITY AGENCY”;

24 (ii) in the matter preceding paragraph
25 (1), by striking “the Secretary” and insert-

1 ing “the Director of the Cybersecurity and
2 Infrastructure Security Agency”;

3 (iii) in paragraph (2)—

4 (I) in subparagraph (A), by in-
5 serting “and reporting requirements
6 under subchapter IV of this title”
7 after “section 3556”; and

8 (II) in subparagraph (D), by
9 striking “the Director or Secretary”
10 and inserting “the Director of the Cy-
11 bersecurity and Infrastructure Secu-
12 rity Agency”;

13 (iv) in paragraph (5), by striking “co-
14 ordinating” and inserting “leading the co-
15 ordination of”;

16 (v) in paragraph (6)—

17 (I) in the matter preceding sub-
18 paragraph (A), by inserting “and
19 verifications specifications” before
20 “promulgated under”;

21 (II) in subparagraph (C), by
22 striking “and” at the end;

23 (III) in subparagraph (D), by
24 adding “and” at the end; and

1 (IV) by adding at the end the fol-
2 lowing:

3 “(E) taking any other action that the Di-
4 rector of the Cybersecurity and Infrastructure
5 Security Agency, in consultation with the Direc-
6 tor—

7 “(i) may determine necessary; and

8 “(ii) is authorized to perform;”;

9 (vi) in paragraph (8), by striking “the
10 Secretary’s discretion” and inserting “the
11 Director of the Cybersecurity and Infra-
12 structure Security Agency’s discretion”;
13 and

14 (vii) in paragraph (9), by striking “as
15 the Director or the Secretary, in consulta-
16 tion with the Director,” and inserting “as
17 the Director of the Cybersecurity and In-
18 frastructure Security Agency”;

19 (C) in subsection (c)—

20 (i) in paragraph (4), by striking
21 “and” at the end;

22 (ii) by redesignating paragraph (5) as
23 paragraph (7); and

24 (iii) by inserting after paragraph (4)
25 the following:

1 “(5) an assessment of agency use of automated
2 verification of standards for the standards promul-
3 gated under section 11331 of title 40 using
4 verification specifications;

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

7 (D) in subsection (f)(2)(B), by striking
8 “conflict with” and inserting “reduce the secu-
9 rity posture of agencies established under”;

10 (E) by redesignating subsections (i), (j),
11 (k), and (l) as subsections (j), (k), (l), and (m)
12 respectively;

13 (F) by inserting after subsection (h) the
14 following:

15 “(i) FEDERAL RISK ASSESSMENTS.—The Director of
16 the Cybersecurity and Infrastructure Security Agency, in
17 coordination with the Director, shall perform, on an ongo-
18 ing and continuous basis, assessments of Federal risk pos-
19 ture using any available information on the cybersecurity
20 posture of agencies, including—

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

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

1 “(3) analysis of incident information under sec-
2 tion 3597;

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

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

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

9 “(7) evaluation of Federal and non-Federal
10 threat intelligence;

11 “(8) data on compliance with standards issued
12 under section 11331 of title 40 that, when appro-
13 priate, uses verification specifications;

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

16 “(10) any other information the Secretary de-
17 termines relevant.”; and

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

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

22 “(1) the specific”;

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

1 (iii) by adding at the end the fol-
2 lowing:

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

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) performing, not less frequently than
15 once every 2 years or based on a significant
16 change to system architecture or security pos-
17 ture, an agency system risk assessment that—

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

21 “(ii) evaluates the data assets inven-
22 toried under section 3511 of title 44 for
23 sensitivity to compromises in confiden-
24 tiality, integrity, and availability;

1 “(iii) identifies agency systems that
2 have access to or hold the data assets
3 inventoried under section 3511 of title 44;

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, based on—

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—

19 (aa) in the matter preceding
20 clause (i), by striking “providing
21 information” and inserting
22 “using information from the as-
23 sessment conducted under sub-
24 paragraph (A), providing, in co-
25 ordination with the Director of

1 the Cybersecurity and Infrastruc-
2 ture Security Agency, informa-
3 tion”;

4 (bb) in clause (i), by striking
5 “and” at the end;

6 (cc) in clause (ii), by adding
7 “and” at the end; and

8 (dd) by adding at the end
9 the following:

10 “(iii) in consultation with the Director
11 and the Director of the Cybersecurity and
12 Infrastructure Security Agency, informa-
13 tion or information systems used by agen-
14 cies through shared services, memoranda
15 of understanding, or other agreements;”;

16 (IV) in subparagraph (C), as so
17 redesignated—

18 (aa) in clause (ii) by insert-
19 ing “binding” before “oper-
20 ational”; and

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

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

1 “(E) not later than 30 days after the date
2 on which an agency system risk assessment is
3 performed under subparagraph (A), providing
4 the assessment to—

5 “(i) the Director;

6 “(ii) the Director of the Cybersecurity
7 and Infrastructure Security Agency; and

8 “(iii) the National Cyber Director;

9 “(F) in consultation with the Director of
10 the Cybersecurity and Infrastructure Security
11 Agency and not less frequently than annually,
12 performing an evaluation of whether additional
13 cybersecurity procedures are appropriate for se-
14 curing a system of, or under the supervision of,
15 the agency, which shall—

16 “(i) be completed considering the
17 agency system risk assessment performed
18 under subparagraph (A); and

19 “(ii) include a specific evaluation for
20 high value assets; and

21 “(G) not later than 30 days after com-
22 pleting the evaluation performed under sub-
23 paragraph (F), providing the evaluation and an
24 implementation plan for using additional cyber-

1 security procedures determined to be appro-
2 priate to—

3 “(i) the Director of the Cybersecurity
4 and Infrastructure Security Agency;

5 “(ii) the Director; and

6 “(iii) the National Cyber Director.”;

7 (ii) in paragraph (2)—

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

13 (II) in subparagraph (B)—

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

17 “(i) standards”; and

18 (bb) by adding at the end
19 the following:

20 “(ii) the evaluation performed under
21 paragraph (1)(F); and

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

24 (III) in subparagraph (D), by in-
25 serting “, through the use of penetra-

1 tion testing, the vulnerability disclo-
2 sure program established under sec-
3 tion 3559B, and other means,” after
4 “periodically”;

5 (iii) in paragraph (3)—

6 (I) in subparagraph (B), by in-
7 serting “, in coordination with the Di-
8 rector of the Cybersecurity and Infra-
9 structure Security Agency,” after
10 “maintaining”;

11 (II) in subparagraph (D), by
12 striking “and” at the end;

13 (III) in subparagraph (E), by
14 adding “and” at the end; and

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

17 “(F) implementing mechanisms for using
18 verification specifications, or alternate
19 verification specifications validated by the Di-
20 rector of the Cybersecurity and Infrastructure
21 Security Agency, in consultation with the Direc-
22 tor of the National Institute of Standards and
23 Technology, to automatically verify the imple-
24 mentation of standards of agency systems pro-
25 mulgated under section 11331 of title 40 or any

1 additional cybersecurity procedures, as applica-
2 ble;”; and

3 (iv) in paragraph (5), by inserting
4 “and the Director of the Cybersecurity and
5 Infrastructure Security Agency” before
6 “on the effectiveness”;

7 (B) in subsection (b)—

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

10 “(1) pursuant to subsection (a)(1)(A), per-
11 forming an agency system risk assessment, which
12 shall include using automated tools consistent with
13 standards, verification specifications, and guidelines
14 promulgated under section 11331 of title 40, as ap-
15 plicable;”;

16 (ii) in paragraph (2)(D)—

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

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

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

1 frastructure Security Agency under section
2 3553 of title 44;” and

3 (III) in clause (iv), as so redesign-
4 nated, by striking “as determined by
5 the agency; and” and inserting “as
6 determined by the agency—

7 “(I) in coordination with the Di-
8 rector of the Cybersecurity and Infra-
9 structure Security Agency; and

10 “(II) in consideration of—

11 “(aa) the agency risk assess-
12 ment performed under subsection
13 (a)(1)(A); and

14 “(bb) the determinations of
15 applying more stringent stand-
16 ards and additional cybersecurity
17 procedures pursuant to section
18 11331(c)(1) of title 40; and”;

19 (iii) in paragraph (5)—

20 (I) in subparagraph (A), by in-
21 serting “, including penetration test-
22 ing, as appropriate,” after “shall in-
23 clude testing”; and

1 (II) in subparagraph (C), by in-
2 serting “, verification specifications,”
3 after “with standards”;

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

11 (v) by redesignating paragraphs (7)
12 and (8) as paragraphs (9) and (10), re-
13 spectively;

14 (vi) by inserting after paragraph (6)
15 the following:

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

22 “(8) a process for providing the verification of
23 the implementation of standards promulgated under
24 section 11331 of title 40 using verification specifica-
25 tions, automation, and machine-readable data, to the

1 Director and the Director of the Cybersecurity and
2 Infrastructure Security Agency;” and

3 (vii) in paragraph (9)(C), as so redesi-
4 gnated—

5 (I) by striking clause (ii) and in-
6 serting the following:

7 “(ii) notifying and consulting with the
8 Federal information security incident cen-
9 ter established under section 3556 pursu-
10 ant to the requirements of section 3594;”;

11 (II) by redesignating clause (iii)
12 as clause (iv);

13 (III) by inserting after clause (ii)
14 the following:

15 “(iii) performing the notifications and
16 other activities required under subchapter
17 IV of this title; and”;

18 (IV) in clause (iv), as so redesi-
19 gnated—

20 (aa) in subclause (I), by
21 striking “and relevant Offices of
22 Inspector General”;

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

1 (cc) by striking subclause
2 (III); and

3 (dd) by redesignating sub-
4 clause (IV) as subclause (III);

5 (C) in subsection (c)—

6 (i) in paragraph (1)—

7 (I) in subparagraph (A)—

8 (aa) in the matter preceding
9 clause (i), by striking “on the
10 adequacy and effectiveness of in-
11 formation security policies, proce-
12 dures, and practices, including”
13 and inserting “that includes”;
14 and

15 (bb) in clause (ii), by insert-
16 ing “unless the Director issues a
17 waiver to the agency under sub-
18 paragraph (B)(iii),” before “the
19 total number”; and

20 (II) by striking subparagraph (B)
21 and inserting the following:

22 “(B) INCIDENT REPORTING WAIVER.—

23 “(i) CERTIFICATION OF AGENCY IN-
24 FORMATION SHARING.—If the Director, in
25 consultation with the Director of the Cy-

1 bersecurity and Infrastructure Security
2 Agency, determines that an agency shares
3 any information relating to any incident
4 pursuant to section 3594(a), the Director
5 shall certify that the agency is in compli-
6 ance with that section.

7 “(ii) CERTIFICATION OF ISSUING RE-
8 PORT.—If the Director determines that the
9 Director of the Cybersecurity and Infra-
10 structure Security Agency uses the infor-
11 mation described in clause (i) with respect
12 to a particular agency to submit to Con-
13 gress an annex required under section
14 3597(c)(3) for that agency, the Director
15 shall certify that the Cybersecurity and In-
16 frastructure Security Agency is in compli-
17 ance with that section with respect to that
18 agency.

19 “(iii) WAIVER.—The Director may
20 waive the reporting requirement with re-
21 spect to the information required to be in-
22 cluded in the report under subparagraph
23 (A)(ii) for a particular agency if—

1 “(I) the Director has issued a
2 certification for the agency under
3 clause (i); and

4 “(II) the Director has issued a
5 certification with respect to the annex
6 of the agency under clause (ii).

7 “(iv) REVOCATION OF WAIVER OR
8 CERTIFICATIONS.—

9 “(I) WAIVER.—If, at any time,
10 the Director determines that the Di-
11 rector of the Cybersecurity and Infra-
12 structure Security Agency cannot sub-
13 mit to Congress an annex for a par-
14 ticular agency under section
15 3597(c)(3)—

16 “(aa) any waiver previously
17 issued under clause (iii) with re-
18 spect to that agency shall be con-
19 sidered void; and

20 “(bb) the Director shall re-
21 voke the certification for the
22 annex of that agency under
23 clause (ii).

24 “(II) CERTIFICATIONS.—If, at
25 any time, the Director determines

1 that an agency has not provided to
2 the Director of the Cybersecurity and
3 Infrastructure Security Agency the to-
4 tality of incident information required
5 under section 3594(a)—

6 “(aa) any waiver previously
7 issued under clause (iii) with re-
8 spect to that agency shall be con-
9 sidered void; and

10 “(bb) the Director shall re-
11 voke the certification for that
12 agency under clause (i).

13 “(III) REISSUANCE.—If the Di-
14 rector revokes a waiver under this
15 clause, the Director may issue a sub-
16 sequent waiver if the Director issues
17 new certifications under clauses (i)
18 and (ii).”;

19 (ii) by redesignating paragraphs (2)
20 through (5) as paragraphs (4) through (7),
21 respectively; and

22 (iii) by inserting after paragraph (1)
23 the following:

24 “(2) BIENNIAL REPORT.—Not later than 180
25 days after the date on which an agency completes an

1 agency system risk assessment under subsection
2 (a)(1)(A) and not less frequently than every 2 years,
3 each agency shall submit to the Director, the Sec-
4 retary, the Committee on Homeland Security and
5 Governmental Affairs of the Senate, the Committee
6 on Oversight and Reform of the House of Represent-
7 atives, the Committee on Homeland Security of the
8 House of Representatives, the appropriate authoriza-
9 tion and appropriations committees of Congress, the
10 National Cyber Director, and the Comptroller Gen-
11 eral of the United States a report that—

12 “(A) summarizes the agency system risk
13 assessment performed under subsection
14 (a)(1)(A);

15 “(B) evaluates the adequacy and effective-
16 ness of information security policies, proce-
17 dures, and practices of the agency to address
18 the risks identified in the system risk assess-
19 ment performed under subsection (a)(1)(A);
20 and

21 “(C) summarizes the evaluations and im-
22 plementation plans described in subparagraphs
23 (F) and (G) of subsection (a)(1) and whether
24 those evaluations and implementation plans call
25 for the use of additional cybersecurity proce-

1 dures determined to be appropriate by the
2 agency.

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

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

8 “(B) may include a classified annex.”; and

9 (D) in subsection (d)(1), in the matter pre-
10 ceding subparagraph (A), by inserting “and the
11 Director of the Cybersecurity and Infrastruc-
12 ture Security Agency” after “the Director”;

13 (4) in section 3555—

14 (A) in subsection (a)(2)(A), by inserting “,
15 including by penetration testing and analyzing
16 the vulnerability disclosure program of the
17 agency” after “information systems”;

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

20 “(f) PROTECTION OF INFORMATION.—(1) Agencies
21 and evaluators shall take appropriate steps to ensure the
22 protection of information which, if disclosed, may ad-
23 versely affect information security.

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 (C) 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 inde-
22 pendent audit under subsection (b).”; and

23 (D) in subsection (j), by striking “the Sec-
24 retary” and inserting “the Director of the

1 Cyber Security and Infrastructure Security
2 Agency”; and

3 (5) in section 3556(a)—

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

8 (B) in paragraph (4), by striking
9 “3554(b)” and inserting “3554(a)(1)(A)”.

10 (d) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

14 “SUBCHAPTER IV—FEDERAL SYSTEM
15 INCIDENT RESPONSE

16 “§ 3591. Definitions

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

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

22 “(1) APPROPRIATE NOTIFICATION ENTITIES.—

23 The term ‘appropriate notification entities’ means—

24 “(A) the Committee on Homeland Security
25 and Governmental Affairs of the Senate;

1 “(B) the Committee on Oversight and Re-
2 form of the House of Representatives;

3 “(C) the Committee on Homeland Security
4 of the House of Representatives;

5 “(D) the appropriate authorization and ap-
6 propriations committees of Congress;

7 “(E) the Director;

8 “(F) the Director of the Cybersecurity and
9 Infrastructure Security Agency;

10 “(G) the National Cyber Director; and

11 “(H) the Comptroller General of the
12 United States.

13 “(2) CONTRACTOR.—The term ‘contractor’—

14 “(A) means any person or business that
15 collects or maintains information that includes
16 personally identifiable information or sensitive
17 personal information on behalf of an agency;
18 and

19 “(B) includes any subcontractor of a per-
20 son or business described in subparagraph (A).

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

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

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

9 **“§ 3592. Notification of high risk exposure after**
10 **major incident**

11 “(a) NOTIFICATION.—As expeditiously as practicable
12 and without unreasonable delay, and in any case not later
13 than 30 days after an agency has a reasonable basis to
14 conclude that a major incident has occurred due to a high
15 risk exposure of personal identifiable information, as de-
16 scribed in section 3598(c)(2), the head of the agency shall
17 provide notice of the major incident in accordance with
18 subsection (b) in writing to the last known home mailing
19 address of each individual whom the major incident may
20 have impacted.

21 “(b) CONTENTS OF NOTICE.—Each notice to an indi-
22 vidual required under subsection (a) shall include—

23 “(1) a description of the rationale for the deter-
24 mination that the major incident resulted in a high

1 risk of exposure of the personal information of the
2 individual;

3 “(2) an assessment of the type of risk the indi-
4 vidual may face as a result of an exposure;

5 “(3) contact information for the Federal Bu-
6 reau of Investigation or other appropriate entity;

7 “(4) the contact information of each nationwide
8 consumer reporting agency;

9 “(5) the contact information for questions to
10 the agency, including a telephone number, e-mail ad-
11 dress, and website;

12 “(6) information on any remedy being offered
13 by the agency;

14 “(7) consolidated Federal Government rec-
15 ommendations on what to do in the event of a major
16 incident; and

17 “(8) any other appropriate information as de-
18 termined by the head of the agency.

19 “(c) DELAY OF NOTIFICATION.—

20 “(1) IN GENERAL.—The Attorney General, the
21 Director of National Intelligence, or the Secretary of
22 Homeland Security may impose a delay of a notifica-
23 tion required under subsection (a) if the notification
24 would disrupt a law enforcement investigation, en-

1 danger national security, or hamper security remedi-
2 ation actions.

3 “(2) DOCUMENTATION.—

4 “(A) IN GENERAL.—Any delay under para-
5 graph (1) shall be reported in writing to the
6 head of the agency, the Director, the Director
7 of the Cybersecurity and Infrastructure Secu-
8 rity Agency, and the Office of Inspector Gen-
9 eral of the agency that experienced the major
10 incident.

11 “(B) CONTENTS.—A statement required
12 under subparagraph (A) shall include a written
13 statement from the entity that delayed the noti-
14 fication explaining the need for the delay.

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

18 “(3) RENEWAL.—A delay under paragraph (1)
19 shall be for a period of 2 months and may be re-
20 newed.

21 “(d) UPDATE NOTIFICATION.—If an agency deter-
22 mines there is a change in the reasonable basis to conclude
23 that a major incident occurred, or that there is a change
24 in the details of the information provided to impacted indi-
25 viduals as described in subsection (b), the agency shall as

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

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

7 “(1) the Director from issuing guidance regard-
8 ing notifications or the head of an agency from
9 sending notifications to individuals impacted by inci-
10 dents not determined to be major incidents; or

11 “(2) the Director from issuing guidance regard-
12 ing notifications of major incidents or the head of an
13 agency from issuing notifications to individuals im-
14 pacted by major incidents that contain more infor-
15 mation than described in subsection (b).

16 **“§ 3593. Congressional notifications and reports**

17 “(a) INITIAL REPORT.—

18 “(1) IN GENERAL.—Not later than 5 days after
19 the date on which an agency has a reasonable basis
20 to conclude that a major incident occurred, the head
21 of the agency shall submit a written notification and,
22 to the extent practicable, provide a briefing, to the
23 appropriate notification entities, taking into ac-
24 count—

1 “(A) the information known at the time of
2 the notification;

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

5 “(C) the classification level of the informa-
6 tion contained in the notification.

7 “(2) CONTENTS.—A notification required under
8 paragraph (1) shall include—

9 “(A) a summary of the information avail-
10 able about the major incident, including how
11 the major incident occurred, based on informa-
12 tion available to agency officials as of the date
13 on which the agency submits the report;

14 “(B) if applicable, an estimate of the num-
15 ber of individuals impacted by the major inci-
16 dent, including an assessment of the risk level
17 to impacted individuals based on the guidance
18 promulgated under section 3598(c)(1) and any
19 information available to agency officials on the
20 date on which the agency submits the report;

21 “(C) if applicable, a description and any
22 associated documentation of any circumstances
23 necessitating a delay in or exemption to notifi-
24 cation granted under subsection (c) or (d) of
25 section 3592; and

1 “(D) if applicable, an assessment of the
2 impacts to the agency, the Federal Government,
3 or the security of the United States, based on
4 information available to agency officials on the
5 date on which the agency submits the report.

6 “(b) SUPPLEMENTAL REPORT.—Within a reasonable
7 amount of time, but not later than 45 days after the date
8 on which additional information relating to a major inci-
9 dent for which an agency submitted a written notification
10 under subsection (a) is discovered by the agency, the head
11 of the agency shall submit to the appropriate notification
12 entities updates to the written notification that include
13 summaries of—

14 “(1) the threats and threat actors,
15 vulnerabilities, means by which the major incident
16 occurred, and impacts to the agency relating to the
17 major incident;

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

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

1 “(4) an estimate of the number of individuals
2 affected by the major incident based on information
3 available to agency officials as of the date on which
4 the agency submits the update;

5 “(5) an update to the assessment of the risk of
6 harm to impacted individuals affected by the major
7 incident based on information available to agency of-
8 ficials as of the date on which the agency submits
9 the update;

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

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

24 “(c) UPDATE REPORT.—If the agency determines
25 that there is any significant change in the understanding

1 of the agency of the scope, scale, or consequence of a
2 major incident for which an agency submitted a written
3 notification under subsection (a), the agency shall provide
4 an updated report to the appropriate notification entities
5 that includes information relating to the change in under-
6 standing.

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

12 “(e) DELAY AND EXEMPTION REPORT.—The Direc-
13 tor shall submit to the appropriate notification entities an
14 annual report on all notification delays and exemptions
15 granted pursuant to subsections (c) and (d) of section
16 3592.

17 “(f) REPORT DELIVERY.—Any written notification or
18 report required to be submitted under this section may
19 be submitted in a paper or electronic format.

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

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

1 “(A) include detailed information about
2 the safeguards that were in place when the inci-
3 dent occurred;

4 “(B) whether the agency implemented the
5 safeguards described in subparagraph (A) cor-
6 rectly; and

7 “(C) in order to protect against a similar
8 incident, identify—

9 “(i) how the safeguards described in
10 subparagraph (A) should be implemented
11 differently; and

12 “(ii) additional necessary safeguards.

13 “(b) COMPLIANCE.—The information provided under
14 subsection (a) shall—

15 “(1) take into account the level of classification
16 of the information and any information sharing limi-
17 tations relating to law enforcement; and

18 “(2) be in compliance with the requirements
19 limiting the release of information under section
20 552a of title 5 (commonly known as the ‘Privacy Act
21 of 1974’).

22 “(c) RESPONDING TO INFORMATION REQUESTS
23 FROM AGENCIES EXPERIENCING INCIDENTS.—An agency
24 that receives a request from another agency or Federal
25 entity for information specifically intended to assist in the

1 remediation or notification requirements due to an inci-
 2 dent shall provide that information to the greatest extent
 3 possible, in accordance with guidance issued by the Direc-
 4 tor and taking into account classification, law enforce-
 5 ment, national security, and compliance with section 552a
 6 of title 5 (commonly known as the ‘Privacy Act of 1974’).

7 “(d) INCIDENT RESPONSE.—Each agency that has a
 8 reasonable basis to conclude that a major incident oc-
 9 curred, regardless of delays from notification granted for
 10 a major incident, shall consult with the Cybersecurity and
 11 Infrastructure Security Agency regarding—

12 “(1) incident response and recovery; and

13 “(2) recommendations for mitigating future in-
 14 cidents.

15 **“§ 3595. Responsibilities of contractors and grant re-
 16 cipients**

17 “(a) NOTIFICATION.—

18 “(1) IN GENERAL.—Subject to paragraph (3),
 19 any contractor of an agency or recipient of a grant
 20 from an agency that has a reasonable basis to con-
 21 clude that an incident involving Federal information
 22 has occurred shall immediately notify the agency.

23 “(2) PROCEDURES.—

24 “(A) MAJOR INCIDENT.—Following notifi-
 25 cation of a major incident by a contractor or re-

1 ipient of a grant under paragraph (1), an
2 agency, in consultation with the contractor or
3 grant recipient, as applicable, shall carry out
4 the requirements under sections 3592, 3593,
5 and 3594 with respect to the major incident.

6 “(B) INCIDENT.—Following notification of
7 an incident by a contractor or recipient of a
8 grant under paragraph (1), an agency, in con-
9 sultation with the contractor or grant recipient,
10 as applicable, shall carry out the requirements
11 under section 3594 with respect to the incident.

12 “(3) APPLICABILITY.—This subsection shall
13 apply to a contractor of an agency or a recipient of
14 a grant from an agency that—

15 “(A) receives information from the agency
16 that the contractor or recipient, as applicable, is
17 not contractually authorized to receive;

18 “(B) experiences an incident relating to
19 Federal information on an information system
20 of the contractor or recipient, as applicable; or

21 “(C) identifies an incident involving a Fed-
22 eral information system.

23 “(b) INCIDENT RESPONSE.—Any contractor of an
24 agency or recipient of a grant from an agency that has
25 a reasonable basis to conclude that a major incident oc-

1 curred shall, in coordination with the agency, consult with
2 the Cybersecurity and Infrastructure Security Agency re-
3 garding—

4 “(1) incident response assistance; and

5 “(2) recommendations for mitigating future in-
6 cidents at the agency.

7 “(c) EFFECTIVE DATE.—This section shall apply on
8 and after the date that is 1 year after the date of enact-
9 ment of the Federal Information Security Modernization
10 Act of 2021.

11 **“§ 3596. Training**

12 “(a) IN GENERAL.—Each agency shall develop train-
13 ing for individuals at the agency with access to Federal
14 information or information systems on how to identify and
15 respond to an incident, including—

16 “(1) the internal process at the agency for re-
17 porting an incident; and

18 “(2) the obligation of the individual to report to
19 the agency a confirmed major incident and any sus-
20 pected incident, involving information in any me-
21 dium or form, including paper, oral, and electronic.

22 “(b) APPLICABILITY.—The training developed under
23 subsection (a) shall—

1 “(1) be required for an individual before the in-
2 dividual may access Federal information or informa-
3 tion systems; and

4 “(2) apply to individuals with temporary access
5 to Federal information or information systems, such
6 as detailees, contractors, subcontractors, grantees,
7 volunteers, and interns.

8 “(c) INCLUSION IN ANNUAL TRAINING.—The train-
9 ing developed under subsection (a) may be included as
10 part of an annual privacy or security awareness training
11 of the agency, as applicable.

12 **“§ 3597. Analysis and report on Federal incidents**

13 “(a) DEFINITION OF COMPROMISE.—In this section,
14 the term ‘compromise’ means—

15 “(1) an incident;

16 “(2) a result of a penetration test in which the
17 tester successfully gains access to a system within
18 the standards under section 3559A;

19 “(3) a vulnerability disclosure; or

20 “(4) any other event that the Director of the
21 Cybersecurity and Infrastructure Security Agency
22 determines identifies an exploitable vulnerability in
23 an agency system.

24 “(b) ANALYSIS OF FEDERAL INCIDENTS.—

1 “(1) IN GENERAL.—The Director of the Cyber-
2 security and Infrastructure Security Agency shall
3 perform continuous monitoring of compromises of
4 agencies.

5 “(2) QUANTITATIVE AND QUALITATIVE ANAL-
6 YSES.—The Director of the Cybersecurity and Infra-
7 structure Security Agency, in consultation with the
8 Director, shall develop and perform continuous mon-
9 itoring and quantitative and qualitative analyses of
10 compromises of agencies, including—

11 “(A) the causes of successful compromises,
12 including—

13 “(i) attacker tactics, techniques, and
14 procedures; and

15 “(ii) system vulnerabilities, including
16 zero days, unpatched systems, and infor-
17 mation system misconfigurations;

18 “(B) the scope and scale of compromises of
19 agencies;

20 “(C) cross Federal Government root causes
21 of compromises of agencies;

22 “(D) agency response, recovery, and reme-
23 diation actions and effectiveness of incidents, as
24 applicable; and

1 “(E) lessons learned and recommendations
2 in responding, recovering, remediating, and
3 mitigating future incidents.

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

8 “(4) SHARING OF DATA AND ANALYSIS.—

9 “(A) IN GENERAL.—The Director shall
10 share on an ongoing basis the analyses required
11 under this subsection with agencies to—

12 “(i) improve the understanding of
13 agencies with respect to risk; and

14 “(ii) support the cybersecurity im-
15 provement efforts of agencies.

16 “(B) FORMAT.—In carrying out subpara-
17 graph (A), the Director shall share the anal-
18 yses—

19 “(i) in human-readable written prod-
20 ucts; and

21 “(ii) to the greatest extent practicable,
22 in machine-readable formats in order to
23 enable automated intake and use by agen-
24 cies.

1 “(c) ANNUAL REPORT ON FEDERAL COM-
2 PROMISES.—Not later than 2 years after the date of en-
3 actment of this section, and not less frequently than annu-
4 ally thereafter, the Director of the Cybersecurity and In-
5 frastructure Security Agency, in consultation with the Di-
6 rector, shall submit to the appropriate notification entities
7 a report that includes—

8 “(1) a summary of causes of compromises from
9 across the Federal Government that categorizes
10 those compromises by the items described in para-
11 graphs (1) through (4) of subsection (a);

12 “(2) the quantitative and qualitative analyses of
13 compromises developed under subsection (b)(2) on
14 an agency-by-agency basis and comprehensively; and

15 “(3) an annex for each agency that includes the
16 total number of compromises of the agency and cat-
17 egorizes those compromises by the items described in
18 paragraphs (1) through (4) of subsection (a).

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

24 “(e) INFORMATION PROVIDED BY AGENCIES.—The
25 analysis required under subsection (b) and each report

1 submitted under subsection (c) shall utilize information
2 provided by agencies pursuant to section 3594(d).

3 “(f) REQUIREMENT TO ANONYMIZE INFORMA-
4 TION.—In publishing the public report required under
5 subsection (d), the Director of the Cybersecurity and In-
6 frastructure Security Agency shall sufficiently anonymize
7 and compile information such that no specific incidents
8 of an agency can be identified, except with the concurrence
9 of the Director of the Office of Management and Budget
10 and in consultation with the impacted agency.

11 **“§ 3598. Major incident guidance**

12 “(a) IN GENERAL.—Not later than 90 days after the
13 date of enactment of the Federal Information Security
14 Management Act of 2021, the Director, in coordination
15 with the Director of the Cybersecurity and Infrastructure
16 Security Agency, shall develop and promulgate guidance
17 on the definition of the term ‘major incident’ for the pur-
18 poses of subchapter II and this subchapter.

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

22 “(1) include, with respect to any information
23 collected or maintained by or on behalf of an agency
24 or an information system used or operated by an

1 agency or by a contractor of an agency or another
2 organization on behalf of an agency—

3 “(A) any incident the head of the agency
4 determines is likely to have an impact on the
5 national security, homeland security, or eco-
6 nomic security of the United States;

7 “(B) any incident the head of the agency
8 determines is likely to have an impact on the
9 operations of the agency, a component of the
10 agency, or the Federal Government, including
11 an impact on the efficiency or effectiveness of
12 agency information systems;

13 “(C) any incident that the head of an
14 agency, in consultation with the Chief Privacy
15 Officer of the agency, determines involves a
16 high risk incident in accordance with the guid-
17 ance issued under subsection (c)(1);

18 “(D) any incident that involves the unau-
19 thorized disclosure of personally identifiable in-
20 formation of not less than 500 individuals, re-
21 gardless of the risk level determined under the
22 guidance issued under subsection (c)(1);

23 “(E) any incident the head of the agency
24 determines involves a high value asset owned or
25 operated by the agency; and

1 “(F) any other type of incident determined
2 appropriate by the Director;

3 “(2) stipulate that every agency shall be consid-
4 ered to have experienced a major incident if the Di-
5 rector of the Cybersecurity and Infrastructure Secu-
6 rity Agency determines that an incident that occurs
7 at not less than 2 agencies—

8 “(A) is enabled by a common technical
9 root cause, such as a supply chain compromise,
10 a common software or hardware vulnerability;
11 or

12 “(B) is enabled by the related activities of
13 a common actor; and

14 “(3) stipulate that, in determining whether an
15 incident constitutes a major incident because that
16 incident—

17 “(A) is any incident described in para-
18 graph (1), the head of an agency shall consult
19 with the Director of the Cybersecurity and In-
20 frastructure Security Agency;

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

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

4 “(i) the Privacy and Civil Liberties
5 Oversight Board; and

6 “(ii) the Executive Director of the
7 Federal Trade Commission.

8 “(c) GUIDANCE ON RISK TO INDIVIDUALS.—

9 “(1) IN GENERAL.—Not later than 90 days
10 after the date of enactment of the Federal Informa-
11 tion Security Modernization Act of 2021, the Direc-
12 tor, in coordination with the Director of the Cyber-
13 security and Infrastructure Security Agency, the
14 Privacy and Civil Liberties Oversight Board, and the
15 Executive Director of the Federal Trade Commis-
16 sion, shall develop and issue guidance to agencies
17 that establishes a risk-based framework for deter-
18 mining the level of risk that an incident involving
19 personally identifiable information could result in
20 substantial harm, physical harm, embarrassment, or
21 unfairness to an individual.

22 “(2) RISK LEVELS AND CONSIDERATIONS.—The
23 risk-based framework included in the guidance
24 issued under paragraph (1) shall—

1 “(A) include a range of risk levels, includ-
2 ing a high risk level; and

3 “(B) consider—

4 “(i) any personally identifiable infor-
5 mation that was exposed as a result of an
6 incident;

7 “(ii) the circumstances under which
8 the exposure of personally identifiable in-
9 formation of an individual occurred; and

10 “(iii) whether an independent evalua-
11 tion of the information affected by an inci-
12 dent determines that the information is
13 unreadable, including, as appropriate, in-
14 stances in which the information is—

15 “(I) encrypted; and

16 “(II) determined by the Director
17 of the Cybersecurity and Infrastruc-
18 ture Security Agency to be of suffi-
19 ciently low risk of exposure.

20 “(3) APPROVAL.—

21 “(A) IN GENERAL.—The guidance issued
22 under paragraph (1) shall include a process by
23 which the Director, jointly with the Director of
24 the Cybersecurity and Infrastructure Security
25 Agency and the Attorney General, may approve

1 the designation of an incident that would be
2 considered high risk as lower risk if information
3 exposed by the incident is unreadable, as de-
4 scribed in paragraph (2)(B)(iii).

5 “(B) DOCUMENTATION.—The Director
6 shall report any approval of an incident granted
7 by the Director under subparagraph (A) to—

8 “(i) the head of the agency that expe-
9 rienced the incident;

10 “(ii) the inspector general of the agen-
11 cy that experienced the incident; and

12 “(iii) the Director of the Cybersecu-
13 rity and Infrastructure Security Agency.

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

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

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

1 “(3) an explanation of, and the analysis that
2 led to, the definition described in paragraph (2); and

3 “(4) an assessment of any additional datasets
4 or risk evaluation criteria that should be included in
5 the risk-based framework included in the guidance
6 issued under subsection (c)(1).”.

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

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification of high risk exposure after major incident.

“3593. Congressional notifications and reports.

“3594. Government information sharing and incident response.

“3595. Responsibilities of contractors and grant recipients.

“3596. Training.

“3597. Analysis and report on Federal incidents.

“3598. Major incident guidance.”.

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

11 (a) INFORMATION TECHNOLOGY MODERNIZATION
12 CENTERS OF EXCELLENCE PROGRAM ACT.—Section
13 2(c)(4)(A)(ii) of the Information Technology Moderniza-
14 tion Centers of Excellence Program Act (40 U.S.C. 11301
15 note) is amended by striking the period at the end and
16 inserting “, which shall be provided in coordination with
17 the Director of the Cybersecurity and Infrastructure Secu-
18 rity Agency.”.

19 (b) MODERNIZING GOVERNMENT TECHNOLOGY.—
20 Subtitle G of title X of Division A of the National Defense

1 Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301
2 note) is amended—

3 (1) in section 1077(b)—

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

7 (B) in paragraph (7)—

8 (i) in the paragraph heading, by strik-
9 ing “CIO” and inserting “CIO”;

10 (ii) by striking “In evaluating
11 projects” and inserting the following:

12 “(A) CONSIDERATION OF GUIDANCE.—In
13 evaluating projects”;

14 (iii) in subparagraph (A), as so des-
15 ignated, by striking “under section
16 1094(b)(1)” and inserting “guidance
17 issued by the Director”; and

18 (iv) by adding at the end the fol-
19 lowing:

20 “(B) CONSULTATION.—In using funds
21 under paragraph (3)(A), the Chief Information
22 Officer of the covered agency shall consult with
23 the Director of the Cybersecurity and Infra-
24 structure Security Agency.”; and

25 (2) in section 1078—

1 (A) by striking subsection (a) and insert-
2 ing the following:

3 “(a) DEFINITIONS.—In this section:

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

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

10 (B) in subsection (b), by adding at the end
11 the following:

12 “(8) PROPOSAL EVALUATION.—The Director
13 shall—

14 “(A) give consideration for the use of
15 amounts in the Fund to improve the security of
16 high value assets; and

17 “(B) require that any proposal for the use
18 of amounts in the Fund includes a cybersecu-
19 rity plan, including a chain risk management
20 plan, to be reviewed by the member of the
21 Technology Modernization Board described in
22 subsection (c)(5)(C).”; and

23 (C) in subsection (c)—

24 (i) in paragraph (2)(A)(i), by insert-
25 ing “, including a consideration of the im-

1 pact on high value assets” after “oper-
2 ational risks”;

3 (ii) in paragraph (5)—

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

6 (II) in subparagraph (B), by
7 striking the period at the end and in-
8 sserting “and”; and

9 (III) by adding at the end the
10 following:

11 “(C) a senior official from the Cybersecu-
12 rity and Infrastructure Security Agency of the
13 Department of Homeland Security, appointed
14 by the Director.”; and

15 (iii) in paragraph (6)(A), by striking
16 “shall be—” and all that follows through
17 “4 employees” and inserting “shall be 4
18 employees”.

19 (c) SUBCHAPTER I.—Subchapter I of subtitle III of
20 title 40, United States Code, is amended—

21 (1) in section 11302—

22 (A) in subsection (b), by striking “use, se-
23 curity, and disposal of” and inserting “use, and
24 disposal, and, in coordination with the Director
25 of the Cybersecurity and Infrastructure Secu-

1 rity Agency, promote and improve the security,
2 of”;

3 (B) in subsection (c)—

4 (i) in paragraph (2), by inserting “in
5 consultation with the Director of the Cy-
6 bersecurity and Infrastructure Security
7 Agency” before “, and results of”;

8 (ii) in paragraph (3)—

9 (I) in subparagraph (A), by strik-
10 ing “, and performance” and inserting
11 “security, and performance”; and

12 (II) in subparagraph (C)—

13 (aa) by striking “For each
14 major” and inserting the fol-
15 lowing:

16 “(i) IN GENERAL.—For each major”;

17 and

18 (bb) by adding at the end
19 the following:

20 “(ii) CYBERSECURITY.—In catego-
21 rizing an investment according to risk
22 under clause (i), the Chief Information Of-
23 ficer of the covered agency shall consult
24 with the Director of the Cybersecurity and

1 Infrastructure Security Agency on the cy-
2 bersecurity or supply chain risk.

3 “(iii) SECURITY RISK GUIDANCE.—
4 The Director, in coordination with the Di-
5 rector of the Cybersecurity and Infrastruc-
6 ture Security Agency, shall issue guidance
7 for the categorization of an investment
8 under clause (i) according to the cyberse-
9 curity or supply chain risk.”; and

10 (iii) in paragraph (4)—

11 (I) in subparagraph (A)—

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

14 (bb) in clause (iii), by strik-
15 ing the period at the end and in-
16 serting “; and”; and

17 (cc) by adding at the end
18 the following:

19 “(iv) in consultation with the Director
20 of the Cybersecurity and Infrastructure Se-
21 curity Agency, the cybersecurity risks of
22 the investment.”; and

23 (II) in subparagraph (B), in the
24 matter preceding clause (i), by insert-
25 ing “not later than 30 days after the

1 date on which the review under sub-
2 paragraph (A) is completed,” before
3 “the Administrator”;

4 (C) in subsection (f)—

5 (i) by striking “heads of executive
6 agencies to develop” and inserting “heads
7 of executive agencies to—

8 “(1) develop”;

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

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

14 “(2) consult with the Director of the Cybersecu-
15 rity and Infrastructure Security Agency for the de-
16 velopment and use of supply chain security best
17 practices.”; and

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

21 (2) in section 11303(b)(2)(B)—

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

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

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

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

5 (d) SUBCHAPTER II.—Subchapter II of subtitle III
6 of title 40, United States Code, is amended—

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

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

12 (3) in section 11317, by inserting “security,”
13 before “or schedule”; and

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

17 (e) SUBCHAPTER III.—Section 11331 of title 40,
18 United States Code, is amended—

19 (1) in subsection (a), by striking “section
20 3532(b)(1)” and inserting “section 3552(b)”;

21 (2) in subsection (b)(1)(A)—

22 (A) by striking “in consultation” and in-
23 serting “in coordination”;

24 (B) by striking “the Secretary of Home-
25 land Security” and inserting “the Director of

1 the Cybersecurity and Infrastructure Security
2 Agency”; and

3 (C) by inserting “and associated
4 verification specifications developed under sub-
5 section (g)” before “pertaining to Federal”;

6 (3) by striking subsection (c) and inserting the
7 following:

8 “(c) APPLICATION OF MORE STRINGENT STAND-
9 ARDS.—

10 “(1) IN GENERAL.—The head of an agency
11 shall—

12 “(A) evaluate the need to employ stand-
13 ards for cost-effective, risk-based information
14 security for all systems, operations, and assets
15 within or under the supervision of the agency
16 that are more stringent than the standards pro-
17 mulgated by the Director under this section, if
18 such standards contain, at a minimum, the pro-
19 visions of those applicable standards made com-
20 pulsory and binding by the Director; and

21 “(B) to the greatest extent practicable and
22 if the head of the agency determines that the
23 standards described in subparagraph (A) are
24 necessary, employ those standards.

1 “(2) EVALUATION OF MORE STRINGENT STAND-
2 ARDS.—In evaluating the need to employ more strin-
3 gent standards under paragraph (1), the head of an
4 agency shall consider available risk information, in-
5 cluding—

6 “(A) the status of cybersecurity remedial
7 actions of the agency;

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

10 “(C) incident information of the agency;

11 “(D) information from—

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

14 “(ii) information from the verification
15 disclosure program established under sec-
16 tion 3559B of title 44;

17 “(E) agency threat hunting results under
18 section 207 of the Federal Information Security
19 Modernization Act of 2021;

20 “(F) Federal and non-Federal threat intel-
21 ligence;

22 “(G) data on compliance with standards
23 issued under this section, using the verification
24 specifications developed under subsection (f)
25 when appropriate;

1 “(H) agency system risk assessments of
2 the agency performed under section
3 3554(a)(1)(A) of title 44; and

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

6 (4) in subsection (d)(2)—

7 (A) by striking the paragraph heading and
8 inserting “CONSULTATION, NOTICE, AND COM-
9 MENT”;

10 (B) by inserting “promulgate,” before
11 “significantly modify”; and

12 (C) by striking “shall be made after the
13 public is given an opportunity to comment on
14 the Director’s proposed decision.” and inserting
15 “shall be made—

16 “(A) for a decision to significantly modify
17 or not promulgate such a proposed standard,
18 after the public is given an opportunity to com-
19 ment on the Director’s proposed decision;

20 “(B) in consultation with the Chief Infor-
21 mation Officers Council, the Director of the Cy-
22 bersecurity and Infrastructure Security Agency,
23 the National Cyber Director, the Comptroller
24 General of the United States, and the Council

1 of the Inspectors General on Integrity and Effi-
2 ciency;

3 “(C) considering the Federal risk assess-
4 ments performed under section 3553(i) of title
5 44; and

6 “(D) considering the extent to which the
7 proposed standard reduces risk relative to the
8 cost of implementation of the standard.”; and

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

10 “(e) REVIEW OF PROMULGATED STANDARDS.—

11 “(1) IN GENERAL.—Not less frequently than
12 once every 2 years, the Director of the Office of
13 Management and Budget, in consultation with the
14 Chief Information Officers Council, the Director of
15 the Cybersecurity and Infrastructure Security Agen-
16 cy, the National Cyber Director, the Comptroller
17 General of the United States, and the Council of the
18 Inspectors General on Integrity and Efficiency shall
19 review the efficacy of the standards in effect promul-
20 gated under this section in reducing cybersecurity
21 risks and determine whether any changes to those
22 standards are appropriate based on—

23 “(A) the Federal risk assessment developed
24 under section 3553(i) of title 44;

25 “(B) public comment; and

1 “(C) an assessment of the extent to which
2 the proposed standards reduce risk relative to
3 the cost of implementation of the standards.

4 “(2) UPDATED GUIDANCE.—Not later than 90
5 days after the date of the completion of the review
6 under paragraph (1), the Director of the Office of
7 Management and Budget shall issue guidance to
8 agencies to make any necessary updates to the
9 standards in effect promulgated under this section
10 based on the results of the review.

11 “(3) CONGRESSIONAL REPORT.—Not later than
12 30 days after the date on which a review is com-
13 pleted under paragraph (1), the Director shall sub-
14 mit to the Committee on Homeland Security and
15 Governmental Affairs of the Senate and the Com-
16 mittee on Oversight and Reform of the House of
17 Representatives a report that includes—

18 “(A) the review of the standards in effect
19 promulgated under this section conducted under
20 paragraph (1);

21 “(B) the risk mitigation offered by each
22 standard described in subparagraph (A); and

23 “(C) a summary of—

1 “(i) the standards to which changes
2 were determined appropriate during the re-
3 view; and

4 “(ii) anticipated changes to the stand-
5 ards under this section in guidance issued
6 under paragraph (2).

7 “(f) VERIFICATION SPECIFICATIONS.—Not later than
8 1 year after the date on which the Director of the National
9 Institute of Standards and Technology issues a proposed
10 standard pursuant to paragraphs (2) and (3) of section
11 20(a) of the National Institute of Standards and Tech-
12 nology Act (15 U.S.C. 278g-3(a)), the Director of the Cy-
13 bersecurity and Infrastructure Security Agency, in con-
14 sultation with the Director of the National Institute of
15 Standards and Technology, as practicable, shall develop
16 technical specifications to enable the automated
17 verification of the implementation of the controls within
18 the standard.”.

19 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**
20 **SPONSE.**

21 (a) RESPONSIBILITIES OF THE CYBERSECURITY AND
22 INFRASTRUCTURE SECURITY AGENCY.—

23 (1) RECOMMENDATIONS.—Not later than 180
24 days after the date of enactment of this Act, the Di-
25 rector of the Cybersecurity and Infrastructure Secu-

1 rity Agency, in coordination with the Chair of the
2 Federal Trade Commission, the Chair of the Securi-
3 ties and Exchange Commission, the Secretary of the
4 Treasury, the Director of the Federal Bureau of In-
5 vestigation, the Director of the National Institute of
6 Standards and Technology, and the head of any
7 other appropriate Federal or non-Federal entity,
8 shall consolidate, maintain, and make publicly avail-
9 able recommendations for individuals whose personal
10 information, as defined in section 3591 of title 44,
11 United States Code, as added by this Act, is inap-
12 propriately exposed as a result of a high risk inci-
13 dent described in section 3598(c)(2) of title 44,
14 United States Code.

15 (2) PLAN FOR ANALYSIS OF, AND REPORT ON,
16 FEDERAL INCIDENTS.—

17 (A) IN GENERAL.—Not later than 180
18 days after the date of enactment of this Act,
19 the Director of the Cybersecurity and Infra-
20 structure Security Agency shall—

21 (i) develop a plan for the development
22 of the analysis required under section
23 3597(b) of title 44, United States Code, as
24 added by this Act, and the report required

1 under subsection (c) of that section that
2 includes—

3 (I) a description of any chal-
4 lenges the Director anticipates en-
5 countering; and

6 (II) the use of automation and
7 machine-readable formats for col-
8 lecting, compiling, monitoring, and
9 analyzing data; and

10 (ii) provide to the appropriate con-
11 gressional committees a briefing on the
12 plan developed under clause (i).

13 (B) BRIEFING.—Not later than 1 year
14 after the date of enactment of this Act, the Di-
15 rector of the Cybersecurity and Infrastructure
16 Security Agency shall provide to the appro-
17 priate congressional committees a briefing on—

18 (i) the execution of the plan required
19 under subparagraph (A); and

20 (ii) the development of the report re-
21 quired under section 3597(c) of title 44,
22 United States Code, as added by this Act.

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

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

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

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

8 (2) INCIDENT DATA SHARING.—

9 (A) IN GENERAL.—The Director shall de-
10 velop guidance, to be updated not less fre-
11 quently than once every 2 years, on the content,
12 timeliness, and format of the information pro-
13 vided by agencies under section 3594(a) of title
14 44, United States Code, as added by this Act.

15 (B) REQUIREMENTS.—The guidance devel-
16 oped under subparagraph (A) shall—

17 (i) prioritize the availability of data
18 necessary to understand and analyze—

19 (I) the causes of incidents;

20 (II) the scope and scale of inci-
21 dents within the agency networks and
22 systems;

23 (III) cross Federal Government
24 root causes of incidents;

1 (IV) agency response, recovery,
2 and remediation actions; and

3 (V) the effectiveness of incidents;

4 (ii) enable the efficient development
5 of—

6 (I) lessons learned and rec-
7 ommendations in responding to, recov-
8 ering from, remediating, and miti-
9 gating future incidents; and

10 (II) the report on Federal com-
11 promises required under section
12 3597(c) of title 44, United States
13 Code, as added by this Act;

14 (iii) include requirements for the time-
15 liness of data production; and

16 (iv) include requirements for using
17 automation and machine-readable data for
18 data sharing and availability.

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

1 (4) STANDARD GUIDANCE AND TEMPLATES.—
2 Not later than 1 year after the date of enactment
3 of this Act, the Director, in coordination with the
4 Director of the Cybersecurity and Infrastructure Se-
5 curity Agency, shall develop guidance and templates,
6 to be reviewed and, if necessary, updated not less
7 frequently than once every 2 years, for use by Fed-
8 eral agencies in the activities required under sections
9 3592, 3593, and 3596 of title 44, United States
10 Code, as added by this Act.

11 (5) CONTRACTOR AND GRANTEE GUIDANCE.—

12 (A) IN GENERAL.—Not later than 1 year
13 after the date of enactment of this Act, the Di-
14 rector, in coordination with the Secretary of
15 Homeland Security, the Secretary of Defense,
16 the Administrator of General Services, and the
17 heads of other agencies determined appropriate
18 by the Director, shall issue guidance to Federal
19 agencies on how to deconflict existing regula-
20 tions, policies, and procedures relating to the
21 responsibilities of contractors and grant recipi-
22 ents established under section 3595 of title 44,
23 United States Code, as added by this Act.

24 (B) EXISTING PROCESSES.—To the great-
25 est extent practicable, the guidance issued

1 under subparagraph (A) shall allow contractors
2 and grantees to use existing processes for noti-
3 fying Federal agencies of incidents involving in-
4 formation of the Federal Government.

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

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

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

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

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

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

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

3 Not later than 1 year after the date of enactment
4 of this Act, the Director, in coordination with the Director
5 of the Cybersecurity and Infrastructure Security Agency,
6 shall issue guidance for agencies on—

7 (1) completing the agency system risk assess-
8 ment required under section 3554(a)(1)(A) of title
9 44, United States Code, as amended by this Act;

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

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

20 (A) specific standards for the automation
21 and machine-readable data; and

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

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

1 (5) implementing standards in agency author-
2 ization processes to encourage the tailoring of proc-
3 esses to agency and system risk that are propor-
4 tionate to the sensitivity of systems, which shall in-
5 clude—

6 (A) a clarification of—

7 (i) the acceptable use and develop-
8 ment of customization of standards pro-
9 mulgated under section 11331 of title 40,
10 United States Code; and

11 (ii) the acceptable use of risk-based
12 authorization procedures authorized on the
13 date of enactment of this Act; and

14 (B) a requirement to coordinate with In-
15 spectors General of agencies to ensure con-
16 sistent understanding and application of agency
17 policies for the purpose of Inspector General
18 audits; and

19 (6) requiring, as practicable and pursuant to
20 section 203, an evaluation of agency cybersecurity
21 using metrics that are—

22 (A) based on outcomes; and

23 (B) based on time.

1 **SEC. 105. AGENCY REQUIREMENTS TO NOTIFY ENTITIES**
2 **IMPACTED BY INCIDENTS.**

3 Not later than 180 days after the date of enactment
4 of this Act, the Director shall issue guidance that requires
5 agencies to notify entities that are compelled to share sen-
6 sitive information with the agency of an incident that im-
7 pacts—

8 (1) sensitive information shared with the agen-
9 cy by the entity; or

10 (2) the systems used to the transmit sensitive
11 information described in paragraph (1) to the agen-
12 cy.

13 **TITLE II—IMPROVING FEDERAL**
14 **CYBERSECURITY**

15 **SEC. 201. EVALUATION OF EFFECTIVENESS OF STANDARDS.**

16 (a) **IN GENERAL.**—As a component of the evaluation
17 and report required under section 3555(h) of title 44,
18 United States Code, and not later than 1 year after the
19 date of enactment of this Act, the Comptroller General
20 of the United States shall perform a study that—

21 (1) assesses the standards promulgated under
22 section 11331(b) of title 40, United States Code to
23 determine the degree to which agencies use the au-
24 thority under section 11331(c)(1) of title 40, United
25 States Code to customize the standards relative to
26 the risks facing each agency and agency system;

1 (2) assesses the effectiveness of the standards
2 described in paragraph (1), including any standards
3 customized by agencies under section 11331(c)(1) of
4 title 40, United States Code, at improving agency
5 cybersecurity;

6 (3) examines the quantification of cybersecurity
7 risk in the private sector for any applicability for use
8 by the Federal Government;

9 (4) examines cybersecurity metrics existing as
10 of the date of enactment of this Act used by the Di-
11 rector, the Director of the Cybersecurity and Infra-
12 structure Security Agency, and the heads of other
13 agencies to evaluate the effectiveness of information
14 security policies and practices; and

15 (5) with respect to the standards described in
16 paragraph (1), provides recommendations for—

17 (A) the addition or removal of standards;

18 or

19 (B) the customization of—

20 (i) the standards by agencies under
21 section 11331(c)(1) of title 40, United
22 States Code; or

23 (ii) specific controls within the stand-
24 ards.

1 (b) INCORPORATION OF STUDY.—The Director shall
2 incorporate the results of the study performed under sub-
3 section (a) into the review of standards required under
4 section 11331(e) of title 40, United States Code.

5 (c) BRIEFING.—Not later than 30 days after the date
6 on which the study performed under subsection (a) is com-
7 pleted, the Comptroller General of the United States shall
8 provide to the appropriate congressional committees a
9 briefing on the study.

10 **SEC. 202. MOBILE SECURITY STANDARDS.**

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

13 (1) evaluate mobile application security stand-
14 ards promulgated under section 11331(b) of title 44,
15 United States Code; and

16 (2) issue guidance to implement mobile security
17 standards in effect on the date of enactment of this
18 Act promulgated under section 11331(b) of title 40,
19 United States Code, including for mobile applica-
20 tions, for every agency.

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

23 (1) a requirement, pursuant to section
24 3506(b)(4) of title 44, United States Code, for every

1 agency to maintain a continuous inventory of
2 every—

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

5 (B) mobile application installed on a mo-
6 bile device described in subparagraph (A); and

7 (C) vulnerability identified by the agency
8 associated with a mobile device or mobile appli-
9 cation described in subparagraphs (A) and (B);
10 and

11 (2) a requirement for every agency to perform
12 continuous evaluation of the vulnerabilities described
13 in paragraph (1)(C) and other risks.

14 (c) INFORMATION SHARING.—The Director, in co-
15 ordination with the Director of the Cybersecurity and In-
16 frastructure Security Agency, shall issue guidance to
17 agencies for sharing the inventory of the agency required
18 under subsection (b)(1) with the Director of the Cyberse-
19 curity and Infrastructure Security Agency, using automa-
20 tion and machine-readable data to the greatest extent
21 practicable.

22 (d) BRIEFING.—Not later than 60 days after the date
23 on which the Director issues guidance under subsection
24 (a)(2), the Director, in coordination with the Director of
25 the Cybersecurity and Infrastructure Security Agency,

1 shall provide to the appropriate congressional committees
2 a briefing on the guidance.

3 **SEC. 203. QUANTITATIVE CYBERSECURITY METRICS.**

4 (a) ESTABLISHING TIME-BASED METRICS.—

5 (1) IN GENERAL.—Not later than 1 year after
6 the date of enactment of this Act, the Director of
7 the Cybersecurity and Infrastructure Security Agen-
8 cy shall—

9 (A) update the metrics used to measure se-
10 curity under section 3554 of title 44, United
11 States Code, including any metrics developed
12 pursuant to section 224(c) of the Cybersecurity
13 Act of 2015 (6 U.S.C. 1522(c)), to include
14 standardized metrics to quantitatively evaluate
15 and identify trends in agency cybersecurity per-
16 formance, including performance for incident
17 response; and

18 (B) evaluate the metrics described in sub-
19 paragraph (A).

20 (2) QUALITIES.—With respect to the updated
21 metrics required under paragraph (1)—

22 (A) not less than 2 of the metrics shall be
23 time-based; and

24 (B) the metrics may include other measur-
25 able outcomes.

1 (3) EVALUATION.—The evaluation required
2 under paragraph (1)(B) shall evaluate—

3 (A) the amount of time it takes for an
4 agency to detect an incident; and

5 (B) the amount of time that passes be-
6 tween—

7 (i) the detection and remediation of
8 an incident; and

9 (ii) the remediation of an incident and
10 the recovery from the incident.

11 (b) IMPLEMENTATION.—

12 (1) IN GENERAL.—The Director, in coordina-
13 tion with the Director of the Cybersecurity and In-
14 frastructure Security Agency, shall promulgate guid-
15 ance that requires the use of the updated metrics de-
16 veloped under subsection (a)(1)(A) by every agency
17 over a 4-year period beginning on the date on which
18 the metrics are developed to track trends in the inci-
19 dent response capabilities of agencies.

20 (2) PENETRATION TESTS.—On not less than 2
21 occasions during the 2-year period following the date
22 on which guidance is promulgated under paragraph
23 (1), not less than 3 agencies shall be subjected to
24 substantially similar penetration tests in order to

1 validate the utility of the metrics developed under
2 subsection (a)(1)(A).

3 (3) DATABASE.—The Director of the Cyberse-
4 curity and Infrastructure Security Agency shall de-
5 velop and use a database that—

6 (A) stores agency metrics information; and

7 (B) allows for the performance of cross-
8 agency comparison of agency incident response
9 capability trends.

10 (c) UPDATED METRICS.—

11 (1) IN GENERAL.—The Director may issue
12 guidance that updates the metrics developed under
13 subsection (a)(1)(A) if the updated metrics—

14 (A) have the qualities described in sub-
15 section (a)(2); and

16 (B) can be evaluated under subsection
17 (a)(3).

18 (2) DATA SHARING.—The guidance issued
19 under paragraph (1) shall require agencies to share
20 with the Director of the Cybersecurity and Infra-
21 structure Security Agency data demonstrating the
22 performance of the agency with the updated metrics
23 included in that guidance against the metrics devel-
24 oped under subsection (a)(1)(A).

25 (d) CONGRESSIONAL REPORTS.—

1 (1) UPDATED METRICS.—Not later than 30
2 days after the date on which the Director of the Cy-
3 bersecurity and Infrastructure Security completes
4 the evaluation required under subsection (a)(1)(B),
5 the Director of the Cybersecurity and Infrastructure
6 Security Agency shall submit to the appropriate con-
7 gressional committees a report on the updated
8 metrics developed under subsection (a)(1)(A).

9 (2) PROGRAM.—Not later than 180 days after
10 the date on which guidance is promulgated under
11 subsection (b)(1), the Director shall submit to the
12 appropriate congressional committees a report on
13 the results of the use of the updated metrics devel-
14 oped under subsection (a)(1)(A) by agencies.

15 **SEC. 204. DATA AND LOGGING RETENTION FOR INCIDENT**
16 **RESPONSE.**

17 (a) RECOMMENDATIONS.—Not later than 60 days
18 after the date of enactment of this Act, the Director of
19 the Cybersecurity and Infrastructure Security Agency, in
20 consultation with the Attorney General and the National
21 Cyber Director, shall submit to the Director recommenda-
22 tions on requirements for logging events on agency sys-
23 tems and retaining other relevant data within the systems
24 and networks of an agency.

1 (b) CONTENTS.—The recommendations provided
2 under subsection (a) shall include—

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

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

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

8 (4) how to ensure the confidentiality, integrity,
9 and availability of logs;

10 (5) requirements to ensure that, upon request,
11 agencies provide logs to—

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

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

17 (6) ensuring the highest level security oper-
18 ations center of each agency has visibility into all
19 agency logs.

20 (c) GUIDANCE.—Not later than 90 days after receiv-
21 ing the recommendations submitted under subsection (a),
22 the Director, in consultation with the Director of the Cy-
23 bersecurity and Infrastructure Security Agency and the
24 Attorney General, shall promulgate guidance to agencies
25 to establish requirements for logging, log retention, log

1 management, and sharing of log data with other appro-
2 priate agencies.

3 (d) PERIODIC REVIEW.—Not later than 2 years after
4 the date on which the Director of the Cybersecurity and
5 Infrastructure Security Agency submits the recommenda-
6 tions required under subsection (a), and not less fre-
7 quently than every 2 years thereafter, the Director of the
8 Cybersecurity and Infrastructure Security Agency, in con-
9 sultation with the Attorney General, shall evaluate the rec-
10 ommendations and provide an update on the recommenda-
11 tions to the Director as necessary.

12 **SEC. 205. CISA AGENCY ADVISORS.**

13 (a) IN GENERAL.—Not later than 120 days after the
14 date of enactment of this Act, the Director of the Cyberse-
15 curity and Infrastructure Security Agency shall assign not
16 less than 1 cybersecurity professional employed by the Cy-
17 bersecurity and Infrastructure Security Agency to be the
18 Cybersecurity and Infrastructure Security Agency advisor
19 to the Chief Information Officer of each agency.

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

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

24 (2) performing risk assessments of agency sys-
25 tems; and

1 (3) other Federal cybersecurity initiatives.

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

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

6 (2) serving as an incident response point of
7 contact between the assigned agency and the Cyber-
8 security and Infrastructure Security Agency; and

9 (3) familiarizing themselves with agency sys-
10 tems, processes, and procedures to better facilitate
11 support to the agency in responding to incidents.

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

14 (e) MULTIPLE ASSIGNMENTS.—One individual advi-
15 sor made be assigned to multiple agency Chief Information
16 Officers under subsection (a).

17 **SEC. 206. FEDERAL PENETRATION TESTING POLICY.**

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

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

22 “(a) DEFINITIONS.—In this section:

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

1 “(2) RULES OF ENGAGEMENT.—The term
2 ‘rules of engagement’ means a set of rules estab-
3 lished by an agency for the use of penetration test-
4 ing.

5 “(b) GUIDANCE.—

6 “(1) IN GENERAL.—Not later than 180 days
7 after the date of enactment of this Act, the Director
8 shall issue guidance that—

9 “(A) requires agencies to use, when and
10 where appropriate, penetration testing on agen-
11 cy systems; and

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

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

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

20 “(i) a shared service of the agency or
21 another agency; or

22 “(ii) an external entity, such as a ven-
23 dor;

24 “(B) include templates and frameworks for
25 reporting the results of penetration testing,

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

3 “(C) require agencies to provide the rules
4 of engagement and results of penetration test-
5 ing to the Director and the Director of the Cy-
6 bersecurity and Infrastructure Security Agency,
7 without regard to the status of the entity that
8 performs the penetration testing.

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

12 “(1) require the agency to perform penetration
13 testing on the high value assets of the agency;

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

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

18 “(B) adverse impacts to operational net-
19 works and systems of the agency; and

20 “(C) inappropriate access to data;

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

24 “(4) include mechanisms for providing consist-
25 ently formatted, and, if applicable, automated and

1 machine-readable, data to the Director and the Di-
2 rector of the Cybersecurity and Infrastructure Secu-
3 rity Agency.

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

7 “(1) establish a certification process for the
8 performance of penetration testing by both Federal
9 and non-Federal entities that establishes minimum
10 quality controls for penetration testing;

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

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

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

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

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

23 “(2) develop and maintain a Federal strategy
24 for the use of penetration testing.

1 “(f) PRIORITIZATION OF PENETRATION TESTING RE-
2 SOURCES.—

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

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

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

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

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

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

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

“3559A. Federal penetration testing.”.

1 (c) PENETRATION TESTING BY THE SECRETARY OF
2 HOMELAND SECURITY.—Section 3553(b) of title 44,
3 United States Code, as amended by section 1705 of the
4 William M. (Mac) Thornberry National Defense Author-
5 ization Act for Fiscal Year 2021 (Public Law 116–283)
6 and section 101, is further amended—

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

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

11 (3) by inserting after paragraph (8) the fol-
12 lowing:

13 “(9) performing penetration testing with or
14 without advance notice to, or authorization from,
15 agencies, to identify vulnerabilities within Federal
16 information systems; and”.

17 **SEC. 207. ONGOING THREAT HUNTING PROGRAM.**

18 (a) THREAT HUNTING PROGRAM.—

19 (1) IN GENERAL.—Not later than 540 days
20 after the date of enactment of this Act, the Director
21 of the Cybersecurity and Infrastructure Security
22 Agency shall establish a program to provide ongoing,
23 hypothesis-driven threat-hunting services on the net-
24 work of each agency.

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

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

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

13 (C) staff threat hunting services;

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

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

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

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

1 (b) REPORTS.—The Director of the Cybersecurity
2 and Infrastructure Security Agency shall submit to the ap-
3 propriate congressional committees—

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

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

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

1 **SEC. 208. CODIFYING VULNERABILITY DISCLOSURE PRO-**
2 **GRAMS.**

3 (a) IN GENERAL.—Chapter 35 of title 44 of United
4 States Code is amended by inserting after section 3559A,
5 as added by section 206 of this Act, the following:

6 **“§ 3559B. Federal vulnerability disclosure programs**

7 “(a) DEFINITIONS.—In this section:

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

11 “(2) REPORTER.—The term ‘reporter’ means
12 an individual that submits a vulnerability report
13 pursuant to the vulnerability disclosure process of an
14 agency.

15 “(b) RESPONSIBILITIES OF OMB.—

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

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

1 “(B) is authorized under the vulnerability
2 disclosure policy developed under subsection
3 (d)(2) of the agency.

4 “(2) SHARING INFORMATION WITH CISA.—The
5 Director, in coordination with the Director of the
6 Cybersecurity and Infrastructure Security Agency,
7 shall issue guidance to agencies on sharing relevant
8 information in a consistent, automated, and machine
9 readable manner with the Cybersecurity and Infra-
10 structure Security Agency, including—

11 “(A) any valid or credible reports of newly
12 discovered or not publicly known vulnerabilities
13 (including misconfigurations) on an agency in-
14 formation system that uses commercial software
15 or services;

16 “(B) information relating to vulnerability
17 disclosure, coordination, or remediation activi-
18 ties of an agency, particularly as those activities
19 relate to outside organizations—

20 “(i) with which the head of the agency
21 believes the Director of the Cybersecurity
22 and Infrastructure Security can assist; or

23 “(ii) about which the head of the
24 agency believes the Director of the Cyber-

1 security and Infrastructure Security should
2 know; and

3 “(C) any other information with respect to
4 which the head of the agency determines helpful
5 or necessary to involve the Cybersecurity and
6 Infrastructure Security Agency.

7 “(3) AGENCY VULNERABILITY DISCLOSURE
8 POLICIES.—

9 “(A) IN GENERAL.—The Director shall
10 issue guidance to agencies on the required min-
11 imum scope of agency systems covered by the
12 vulnerability disclosure policy of an agency re-
13 quired under subsection (d)(2).

14 “(B) DEADLINE.—Not later than 2 years
15 after the date of enactment of the Federal In-
16 formation Security Modernization Act of 2021,
17 the Director shall update the guidance issued
18 under subparagraph (A) to require that every
19 agency system that is connected to the internet
20 is covered by the vulnerability disclosure policy
21 of the agency.

22 “(c) RESPONSIBILITIES OF CISA.—The Director of
23 the Cybersecurity and Infrastructure Security Agency
24 shall—

1 “(1) provide support to agencies with respect to
2 the implementation of the requirements of this sec-
3 tion;

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

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

11 “(d) RESPONSIBILITIES OF AGENCIES.—

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

16 “(A) an appropriate security contact; and

17 “(B) the component of the agency that is
18 responsible for the internet accessible services
19 offered at the domain.

20 “(2) VULNERABILITY DISCLOSURE POLICY.—

21 The head of each agency shall develop and make
22 publicly available a vulnerability disclosure policy for
23 the agency, which shall—

24 “(A) describe—

1 “(i) the scope of the systems of the
2 agency included in the vulnerability disclo-
3 sure policy;

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

6 “(iii) the type of information system
7 testing that is not authorized by the agen-
8 cy; and

9 “(iv) the disclosure policy of the agen-
10 cy for sensitive information;

11 “(B) include a provision that authorizes
12 the anonymous submission of a vulnerability by
13 a reporter;

14 “(C) 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 under subparagraph (B), when the re-
20 porter should anticipate an acknowledg-
21 ment of receipt of the report by the agen-
22 cy; and

23 “(D) include any other relevant informa-
24 tion.

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

6 “(e) PAPERWORK REDUCTION ACT EXEMPTION.—
7 The requirements of subchapter I (commonly known as
8 the ‘Paperwork Reduction Act’) shall not apply to a vul-
9 nerability disclosure program established under this sec-
10 tion.

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

23 (b) CLERICAL AMENDMENT.—The table of sections
24 for chapter 35 of title 44, United States Code, is amended

1 by adding after the item relating to section 3559A the fol-
2 lowing:

“3559B. Federal vulnerability disclosure programs.”.

3 **SEC. 209. IMPLEMENTING PRESUMPTION OF COMPROMISE**
4 **AND ZERO TRUST ARCHITECTURES.**

5 (a) RECOMMENDATIONS.—Not later than 60 days
6 after the date of enactment of this Act, the Director of
7 the Cybersecurity and Infrastructure Security Agency, in
8 consultation with the Director of the National Institute
9 of Standards and Technology, shall develop recommenda-
10 tions to increase the internal defenses of agency systems
11 to—

12 (1) limit the ability of entities that cause inci-
13 dents to move laterally through or between agency
14 systems;

15 (2) identify incidents more quickly;

16 (3) isolate and remove unauthorized entities
17 from agency systems more quickly;

18 (4) implement zero trust architecture; and

19 (5) otherwise increase the resource costs for en-
20 tities that cause incidents; and

21 (b) OMB GUIDANCE.—Not later than 180 days after
22 the date on which the recommendations under subsection
23 (a) are completed, the Director shall issue guidance to
24 agencies that requires the implementation of the rec-
25 ommendations.

1 (c) AGENCY IMPLEMENTATION PLANS.—Not later
2 than 60 days after the date on which the Director issues
3 guidance under subsection (b), the head of each agency
4 shall submit to the Director a plan to implement zero trust
5 architecture that includes—

6 (1) a description of any steps the agency has
7 completed;

8 (2) an identification of activities that will have
9 the most immediate security impact; and

10 (3) a schedule to implement the plan.

11 (d) REPORT AND BRIEFING.—Not later than 90 days
12 after the date on which the Director issues guidance re-
13 quired under subsection (b), the Director shall provide a
14 briefing to the appropriate congressional committees on
15 the guidance and the agency implementation plans sub-
16 mitted under subsection (c).

17 **SEC. 210. AUTOMATION REPORTS.**

18 (a) OMB REPORT.—Not later than 180 days after
19 the date of enactment of this Act, the Director shall sub-
20 mit to the appropriate congressional committees a report
21 on the use of automation under paragraphs (1), (5)(C)
22 and (7)(B) of section 3554(b) of title 44, United States
23 Code.

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

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

6 **SEC. 211. EXTENSION OF FEDERAL ACQUISITION SECURITY**
7 **COUNCIL.**

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

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

14 **SEC. 301. CONTINUOUS INDEPENDENT FISMA EVALUATION**
15 **PILOT.**

16 (a) **IN GENERAL.**—Not later than 2 years after the
17 date of enactment of this Act, the Director, in coordina-
18 tion with the Director of the Cybersecurity and Infrastruc-
19 ture Security Agency, shall establish a pilot program to
20 perform continual agency auditing of the standards pro-
21 mulgated under section 11331 of title 40, United States
22 Code.

23 (b) **PURPOSE.**—

24 (1) **IN GENERAL.**—The purpose of the pilot
25 program established under subsection (a) shall be to

1 develop the capability to continuously audit agency
2 cybersecurity postures, rather than performing an
3 annual audit.

4 (2) USE OF INFORMATION.—It is the sense of
5 Congress that information relating to agency cyber-
6 security postures should be used, on an ongoing
7 basis, to increase agency understanding of cyberse-
8 curity risk and improve agency cybersecurity.

9 (c) PARTICIPATING AGENCIES.—

10 (1) IN GENERAL.—The Director, in coordina-
11 tion with the Council of the Inspectors General on
12 Integrity and Efficiency and in consultation with the
13 Director of the Cybersecurity and Infrastructure Se-
14 curity Agency, shall identify not less than 1 agency
15 and the Inspector General of each identified agency
16 to participate in the pilot program established under
17 subsection (a).

18 (2) CAPABILITIES OF AGENCY.—An agency se-
19 lected under paragraph (1) shall have advanced cy-
20 bersecurity capabilities, including the capability to
21 implement verification specifications and other auto-
22 mated and machine-readable means of sharing infor-
23 mation.

24 (3) CAPABILITIES OF INSPECTOR GENERAL.—
25 The Inspector General of an agency selected under

1 paragraph (1) shall have advanced cybersecurity ca-
2 pabilities, including the ability—

3 (A) to perform real-time or almost real-
4 time and continuous analysis of the use of
5 verification specifications by the agency to as-
6 sess compliance with standards promulgated
7 under section 11331 of title 40, United States
8 Code; and

9 (B) to assess the impact and deployment
10 of additional cybersecurity procedures.

11 (d) DUTIES.—The Director, in coordination with the
12 Council of the Inspectors General on Integrity and Effi-
13 ciency, the Director of the Cybersecurity and Infrastruc-
14 ture Security Agency, and the head of each agency partici-
15 pating in the pilot program under subsection (c), shall de-
16 velop processes and procedures to perform a continuous
17 independent evaluation of—

18 (1) the compliance of the agency with—

19 (A) the standards promulgated under sec-
20 tion 11331 of title 40, United States Code,
21 using verification specifications to the greatest
22 extent practicable; and

23 (B) any additional cybersecurity proce-
24 dures implemented by the agency as a result of
25 the evaluation performed under section

1 3554(a)(1)(F) of title 44, United States Code;
2 and

3 (2) the overall cybersecurity posture of the
4 agency, which may include an evaluation of—

5 (A) the status of cybersecurity remedial ac-
6 tions of the agency;

7 (B) any vulnerability information relating
8 to agency systems that is known to the agency;

9 (C) incident information of the agency;

10 (D) penetration testing performed by an
11 external entity under section 3559A of title 44,
12 United States Code;

13 (E) information from the vulnerability dis-
14 closure program information established under
15 section 3559B of title 44, United States Code;

16 (F) agency threat hunting results; and

17 (G) any other information determined rel-
18 evant by the Director.

19 (e) INDEPENDENT EVALUATION WAIVER.—With re-
20 spect to an agency that participates in the pilot program
21 under subsection (a) during any year other than the first
22 year during which the pilot program is conducted, the Di-
23 rector, with the concurrence of the Director of the Cyber-
24 security and Infrastructure Security Agency, may waive
25 any requirement of the agency with respect to the annual

1 independent evaluation under section 3555 of title 44,
2 United States Code.

3 (f) DURATION.—The pilot program established under
4 this section—

5 (1) shall be performed over a period of not less
6 than 2 years at each agency that participates in the
7 pilot program under subsection (c), unless the Direc-
8 tor, in consultation with the Director of the Cyberse-
9 curity and Infrastructure Security Agency and the
10 Council of the Inspectors General on Integrity and
11 Efficiency, determines that continuing the pilot pro-
12 gram would reduce the cybersecurity of the agency;
13 and

14 (2) may be extended by the Director, in con-
15 sultation with the Director of the Cybersecurity and
16 Infrastructure Security Agency and the Council of
17 the Inspectors General on Integrity and Efficiency,
18 if the Director makes the determination described in
19 paragraph (1).

20 (g) REPORTS.—

21 (1) PILOT PROGRAM PLAN.—Before identifying
22 any agencies to participate in the pilot program
23 under subsection (c), the Director, in coordination
24 with the Director of the Cybersecurity and Infra-
25 structure Security Agency and the Council of the In-

1 spectors General on Integrity and Efficiency, shall
2 submit to the appropriate congressional committees
3 a plan for the pilot program that outlines selection
4 criteria and preliminary plans to implement the pilot
5 program.

6 (2) BRIEFING.—Before commencing a contin-
7 uous independent evaluation of any agency under
8 the pilot program established under subsection (a),
9 the Director shall provide to the appropriate con-
10 gressional committees a briefing on—

11 (A) the selection of agencies to participate
12 in the pilot program; and

13 (B) processes and procedures to perform a
14 continuous independent evaluation of agencies.

15 (3) PILOT RESULTS.—Not later than 60 days
16 after the final day of each year during which an
17 agency participates in the pilot program established
18 under subsection (a), the Director, in coordination
19 with the Director of the Cybersecurity and Infra-
20 structure Security Agency and the Council of the In-
21 spectors General on Integrity and Efficiency, shall
22 submit to the appropriate congressional committees
23 a report on the results of the pilot program for each
24 agency that participates in the pilot program during
25 that year.

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

2 (a) DEFINITION.—In this section, the term “active
3 defense technique”—

4 (1) means an action taken on the systems of an
5 entity to increase the security of information on the
6 network of an agency by misleading an adversary;
7 and

8 (2) includes a honeypot, deception, or purpose-
9 fully feeding false or misleading data to an adver-
10 sary when the adversary is on the systems of the en-
11 tity.

12 (b) STUDY.—Not later than 180 days after the date
13 of enactment of this Act, the Director of the Cybersecurity
14 and Infrastructure Security Agency shall perform a study
15 on the use of active defense techniques to enhance the se-
16 curity of agencies, which shall include—

17 (1) a review of legal restrictions on the use of
18 different active cyber defense techniques on Federal
19 networks;

20 (2) an evaluation of—

21 (A) the efficacy of a selection of active de-
22 fense techniques determined by the Director of
23 the Cybersecurity and Infrastructure Security
24 Agency; and

1 (B) factors that impact the efficacy of the
2 active defense techniques evaluated under sub-
3 paragraph (A); and

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

6 (c) PILOT PROGRAM.—Not later than 180 days after
7 the date of enactment of this Act, the Director, in coordi-
8 nation with the Director of the Cybersecurity and Infra-
9 structure Security Agency, shall establish a pilot program
10 at not less than 2 agencies to implement, and assess the
11 effectiveness of, not less than 1 active cyber defense tech-
12 nique.

13 (d) PURPOSE.—The purpose of the pilot program es-
14 tablished under subsection (c) shall be to—

15 (1) identify any statutory or policy limitations
16 on using active defense techniques;

17 (2) understand the efficacy of using active de-
18 fense techniques; and

19 (3) implement the use of effective techniques to
20 improve agency systems.

21 (e) PLAN.—Not later than 360 days after the date
22 of enactment of this Act, the Director of the Cybersecurity
23 and Infrastructure Security Agency, in coordination with
24 the Director, shall develop a plan to offer any active de-
25 fense technique determined to be successful during the

1 pilot program established under subsection (c) as a shared
2 service to other agencies.

3 (f) REPORTS.—Not later than 1 year after the date
4 of enactment of this Act, the Director of the Cybersecurity
5 and Infrastructure Security Agency shall—

6 (1) provide to the appropriate congressional
7 committees a briefing on—

8 (A) the results of the study performed
9 under subsection (b); and

10 (B) the agencies selected to participate in
11 the pilot program established under subsection
12 (c);

13 (2) submit to the appropriate congressional
14 committees a report on the results of the pilot pro-
15 gram established under subsection (c), including any
16 recommendations developed from the results of the
17 pilot program; and

18 (3) submit to the appropriate congressional
19 committees a copy of the plan developed under sub-
20 section (e).

21 (g) SUNSET.—

22 (1) IN GENERAL.—The requirements of this
23 section shall terminate on the date that is 3 years
24 after the date of enactment of this Act.

1 (2) **AUTHORITY TO CONTINUE USE OF TECH-**
2 **NIQUES.**—Notwithstanding paragraph (1), after the
3 date described in paragraph (1), the Director of the
4 Cybersecurity and Infrastructure Security Agency
5 may continue to offer any active defense technique
6 determined to be successful during the pilot program
7 established under subsection (c) as a shared service
8 to agencies.

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

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

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

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

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

3 (2) staffing and resources; and

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

6 (d) PILOT PROGRAM.—

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

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

21 (e) BRIEFING AND REPORT.—

22 (1) BRIEFING.—Not later than 260 days after
23 the date of enactment of this Act, the Director of
24 the Cybersecurity and Infrastructure Security Agen-
25 cy shall provide to the Committee on Homeland Se-

1 security and Governmental Affairs of the Senate and
2 the Committee on Homeland Security and the Com-
3 mittee on Oversight and Reform of the House of
4 Representatives a briefing on the parameters of any
5 1-year agreements entered into under subsection
6 (d)(1).

7 (2) REPORT.—Not later than 90 days after the
8 date on which the first 1-year agreement entered
9 into under subsection (d) expires, the Director of the
10 Cybersecurity and Infrastructure Security Agency
11 shall submit to the Committee on Homeland Secu-
12 rity and Governmental Affairs of the Senate and the
13 Committee on Homeland Security and the Com-
14 mittee on Oversight and Reform of the House of
15 Representatives a report on—

16 (A) the agreement; and

17 (B) any additional agreements entered into
18 with agencies under subsection (d).

○