

Calendar No. 673

117TH CONGRESS
2D SESSION**S. 2902****[Report No. 117-274]**

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

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 29, 2021

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

DECEMBER 19, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

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~~”.

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

2 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.

3 **SEC. 3. DEFINITIONS.**

4 In this Act, unless otherwise specified:

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

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

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

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

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

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

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

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

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

23 (7) THREAT HUNTING.—The term “threat
24 hunting” means proactively and iteratively searching

1 for threats to systems that evade detection by auto-
2 mated threat detection systems.

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

7 **TITLE I—UPDATES TO FISMA**

8 **SEC. 101. TITLE 44 AMENDMENTS.**

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

11 (1) in section 3504—

12 (A) in subsection (a)(1)(B)(v), by striking
13 “confidentiality, security, disclosure, and shar-
14 ing of information” and inserting “disclosure,
15 sharing of information, and, in consultation
16 with the Director of the Cybersecurity and In-
17 frastructure Security Agency, confidentiality
18 and security”;

19 (B) in subsection (b)(2)(B), by inserting
20 “in coordination with the Director of the Cyber-
21 security and Infrastructure Security Agency”
22 after “standards for security”;

23 (C) in subsection (g), by striking para-
24 graph (1) and inserting the following:

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

3 “(A) develop and oversee the implementa-
4 tion of policies, principles, standards, and
5 guidelines on privacy, disclosure, and sharing of
6 the information; and

7 “(B) in consultation with the Director of
8 the Cybersecurity and Infrastructure Security
9 Agency, develop and oversee policies, principles,
10 standards, and guidelines on confidentiality and
11 security of the information; and”;

12 (D) in subsection (h)(1)—

13 (i) in the matter preceding subpara-
14 graph (A)—

15 (I) by inserting “the Director of
16 the Cybersecurity and Infrastructure
17 Security Agency,” before “the Direc-
18 tor”;

19 (II) by inserting a comma before
20 “and the Administrator”;

21 (ii) in subparagraph (A), by inserting
22 “security and” after “information tech-
23 nology”;

24 (2) in section 3505—

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

3 (i) in subparagraph (B)—

4 (I) by inserting “and the Direc-
5 tor of the Cybersecurity and Infra-
6 structure Security Agency” after
7 “Comptroller General”; and

8 (II) by striking “and” at the end;

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

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

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

17 (B) by striking the second subsection des-
18 ignated as subsection (c);

19 (3) in section 3506—

20 (A) in subsection (b)—

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

23 (ii) in paragraph (4), by inserting
24 “the Director of the Cybersecurity and In-

1 frastructure Security Agency,” after “Gen-
2 eral Services,”; and

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

5 (4) in section 3513—

6 (A) in subsection (a), by inserting “the Di-
7 rector of the Cybersecurity and Infrastructure
8 Security Agency,” before “the Administrator of
9 General Services”;

10 (B) by redesignating subsection (c) as sub-
11 section (d); and

12 (C) by inserting after subsection (b) the
13 following:

14 “(e) Each agency providing a written plan under sub-
15 section (b) shall provide any portion of the written plan
16 addressing information security or cybersecurity to the Di-
17 rector of the Cybersecurity and Infrastructure Security
18 Agency.”; and

19 (5) in section 3520A(b)—

20 (A) in paragraph (1), by striking “, protec-
21 tion”;

22 (B) by redesignating paragraphs (2), (3),
23 (4), and (5) as paragraphs (3), (4), (5), and
24 (6), respectively; and

1 (C) by inserting after paragraph (1) the
2 following:

3 “~~(2) in consultation with the Director of the~~
4 ~~Cybersecurity and Infrastructure Security Agency,~~
5 ~~establish Governmentwide best practices for the pro-~~
6 ~~tection of data;”.~~

7 (b) SUCH CHAPTER II DEFINITIONS.—

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

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

13 (B) by inserting before paragraph (2), as
14 so redesignated, the following:

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

24 (C) by inserting after paragraph (6), as so
25 redesignated, the following:

1 “(7) The term ‘high value asset’ means infor-
2 mation or an information system that the head of an
3 agency determines so critical to the agency that the
4 loss or corruption of the information or the loss of
5 access to the information system would have a seri-
6 ous impact on the ability of the agency to perform
7 the mission of the agency or conduct business.

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

11 (D) by inserting after paragraph (9), as so
12 redesignated, the following:

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

15 “(A) is conducted on an information sys-
16 tem or a component of an information system;
17 and

18 “(B) emulates an attack or other exploi-
19 tation capability of a potential adversary, typi-
20 cally under specific constraints, in order to
21 identify any vulnerabilities of an information
22 system or a component of an information sys-
23 tem that could be exploited.”; and

24 (E) by inserting after paragraph (11), as
25 so redesignated, the following:

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

4 “(13) The term ‘verification specification’
5 means a specification developed under section
6 11331(f) of title 40.”.

7 (2) CONFORMING AMENDMENTS.—

8 (A) HOMELAND SECURITY ACT OF 2002.—

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

13 (B) TITLE 10.—

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

18 (ii) SECTION 2223.—Section
19 2223(c)(3) of title 10, United States Code,
20 is amended by striking “section
21 3552(b)(6)” and inserting “section
22 3552(b)”.

23 (iii) SECTION 2315.—Section 2315 of
24 title 10, United States Code, is amended

1 by striking “section 3552(b)(6)” and in-
2 serting “section 3552(b)”.

3 (iv) SECTION 2339A.—Section
4 2339a(e)(5) of title 10, United States
5 Code, is amended by striking “section
6 3552(b)(6)” and inserting “section
7 3552(b)”.

8 (C) HIGH-PERFORMANCE COMPUTING ACT
9 OF 1991.—Section 207(a) of the High-Perform-
10 ance Computing Act of 1991 (15 U.S.C.
11 5527(a)) is amended by striking “section
12 3552(b)(6)(A)(i)” and inserting “section
13 3552(b)(9)(A)(i)”.

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

20 (E) NATIONAL DEFENSE AUTHORIZATION
21 ACT FOR FISCAL YEAR 2013.—Section
22 933(e)(1)(B) of the National Defense Author-
23 ization Act for Fiscal Year 2013 (10 U.S.C.
24 2224 note) is amended by striking “section
25 3542(b)(2)” and inserting “section 3552(b)”.

1 (F) ~~IKE SKELTON NATIONAL DEFENSE AU-~~
2 ~~THORIZATION ACT FOR FISCAL YEAR 2011.~~—The
3 ~~Ike Skelton National Defense Authorization Act~~
4 ~~for Fiscal Year 2011 (Public Law 111-383) is~~
5 ~~amended—~~

6 (i) in section 806(c)(5) (10 U.S.C.
7 2304 note), by striking “section 3542(b)”
8 and inserting “section 3552(b)”;

9 (ii) in section 931(b)(3) (10 U.S.C.
10 2223 note), by striking “section
11 3542(b)(2)” and inserting “section
12 3552(b)”;

13 (iii) in section 932(b)(2) (10 U.S.C.
14 2224 note), by striking “section
15 3542(b)(2)” and inserting “section
16 3552(b)”.

17 (G) ~~E-GOVERNMENT ACT OF 2002.~~—Sec-
18 ~~tion 301(e)(1)(A) of the E-Government Act of~~
19 ~~2002 (44 U.S.C. 3501 note) is amended by~~
20 ~~striking “section 3542(b)(2)” and inserting~~
21 ~~“section 3552(b)”.~~

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

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

4 (ii) in subsection (f)—

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

8 (II) in paragraph (5), by striking
 9 “section 3532(b)(2)” and inserting
 10 “section 3552(b)”.

11 (e) SUBCHAPTER H AMENDMENTS.—Subchapter H
 12 of chapter 35 of title 44, United States Code, is amend-
 13 ed—

14 (1) in section 3551—

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

18 (B) by inserting after paragraph (2) the
 19 following:

20 “(3) recognize the role of the Cybersecurity and
 21 Infrastructure Security Agency as the lead cyberse-
 22 curity entity for operational coordination across the
 23 Federal Government;”;

1 (C) in paragraph (5), as so redesignated,
2 by striking “diagnose and improve” and insert-
3 ing “integrate, deliver, diagnose, and improve”;

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

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

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

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

16 “(10) recognize that—

17 “(A) a holistic Federal cybersecurity model
18 is necessary to account for differences between
19 the missions and capabilities of agencies; and

20 “(B) in accounting for the differences de-
21 scribed in subparagraph (A) and ensuring over-
22 all Federal cybersecurity—

23 “(i) the Office of Management and
24 Budget is the leader for policy development
25 and oversight of Federal cybersecurity;

1 “(ii) the Cybersecurity and Infrastruc-
 2 ture Security Agency is the leader for im-
 3 plementing operations at agencies; and

4 “(iii) the National Cyber Director is
 5 responsible for developing the overall cy-
 6 bersecurity strategy of the United States
 7 and advising the President on matters re-
 8 lating to cybersecurity.”;

9 ~~(2) in section 3553, as amended by section~~
 10 ~~1705 of the William M. (Mac) Thornberry National~~
 11 ~~Defense Authorization Act for Fiscal Year 2021~~
 12 ~~(Public Law 116-283)—~~

13 ~~(A) in subsection (a)—~~

14 ~~(i) in paragraph (1)—~~

15 ~~(I) by striking “developing and”~~
 16 ~~and inserting “in coordination with~~
 17 ~~the Director of the Cybersecurity and~~
 18 ~~Infrastructure Security Agency,”; and~~

19 ~~(II) by inserting “and associated~~
 20 ~~verification specifications” before~~
 21 ~~“promulgated”; and~~

22 ~~(ii) in paragraph (5), by inserting “,~~
 23 ~~in coordination with the Director of the~~
 24 ~~Cybersecurity and Infrastructure Security~~
 25 ~~Agency,” before “agency compliance”;~~

1 (B) in subsection (b)—

2 (i) by striking the subsection heading
3 and inserting “CYBERSECURITY AND IN-
4 FRASTRUCTURE SECURITY AGENCY”;

5 (ii) in the matter preceding paragraph
6 (1), by striking “the Secretary” and insert-
7 ing “the Director of the Cybersecurity and
8 Infrastructure Security Agency”;

9 (iii) in paragraph (2)—

10 (I) in subparagraph (A), by in-
11 sserting “and reporting requirements
12 under subchapter IV of this title”
13 after “section 3556”; and

14 (II) in subparagraph (D), by
15 striking “the Director or Secretary”
16 and inserting “the Director of the Cy-
17 bersecurity and Infrastructure Secu-
18 rity Agency”;

19 (iv) in paragraph (5), by striking “co-
20 ordinating” and inserting “leading the co-
21 ordination of”;

22 (v) in paragraph (6)—

23 (I) in the matter preceding sub-
24 paragraph (A), by inserting “and

1 verifications specifications” before
2 “promulgated under”;

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

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

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

9 “(E) taking any other action that the Di-
10 rector of the Cybersecurity and Infrastructure
11 Security Agency, in consultation with the Direc-
12 tor—

13 “(i) may determine necessary; and

14 “(ii) is authorized to perform;”;

15 (vi) in paragraph (8), by striking “the
16 Secretary’s discretion” and inserting “the
17 Director of the Cybersecurity and Infra-
18 structure Security Agency’s discretion”;
19 and

20 (vii) in paragraph (9), by striking “as
21 the Director or the Secretary, in consulta-
22 tion with the Director,” and inserting “as
23 the Director of the Cybersecurity and In-
24 frastructure Security Agency”;

25 (C) in subsection (c)—

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

3 (ii) by redesignating paragraph (5) as
4 paragraph (7); and

5 (iii) by inserting after paragraph (4)
6 the following:

7 “(5) an assessment of agency use of automated
8 verification of standards for the standards promul-
9 gated under section 11331 of title 40 using
10 verification specifications;

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

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

16 (E) by redesignating subsections (i), (j),
17 (k), and (l) as subsections (j), (k), (l), and (m)
18 respectively;

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

21 “(i) FEDERAL RISK ASSESSMENTS.—The Director of
22 the Cybersecurity and Infrastructure Security Agency, in
23 coordination with the Director, shall perform, on an ongo-
24 ing and continuous basis, assessments of Federal risk pos-

1 ture using any available information on the cybersecurity
2 posture of agencies, including—

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

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

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

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

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

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

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

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

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

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

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

1 (i) by striking “regarding the spe-
2 cific” and inserting “that includes a sum-
3 mary of—

4 “(1) the specific”;

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

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

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

12 (3) in section 3554—

13 (A) in subsection (a)—

14 (i) in paragraph (1)—

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

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

21 “(A) performing, not less frequently than
22 once every 2 years or based on a significant
23 change to system architecture or security pos-
24 ture, an agency system risk assessment that—

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

4 “(ii) evaluates the data assets inven-
5 toried under section 3511 of title 44 for
6 sensitivity to compromises in confiden-
7 tiality, integrity, and availability;

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

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

16 “(v) evaluates the vulnerability of
17 agency systems and data, including high
18 value assets, based on—

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

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

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

5 “~~(IV)~~ incidents; and

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

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

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

22 ~~(III)~~ in subparagraph ~~(B)~~; as so
23 redesignated—

24 ~~(aa)~~ in the matter preceding
25 clause ~~(i)~~, by striking “providing

1 information” and inserting
2 “using information from the as-
3 sessment conducted under sub-
4 paragraph (A), providing, in co-
5 ordination with the Director of
6 the Cybersecurity and Infrastruc-
7 ture Security Agency, informa-
8 tion”;

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

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

13 (dd) by adding at the end
14 the following:

15 “(iii) in consultation with the Director
16 and the Director of the Cybersecurity and
17 Infrastructure Security Agency, informa-
18 tion or information systems used by agen-
19 cies through shared services, memoranda
20 of understanding, or other agreements;”;

21 (IV) in subparagraph (C), as so
22 redesignated—

23 (aa) in clause (ii) by insert-
24 ing “binding” before “oper-
25 ational”; and

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

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

5 “(E) not later than 30 days after the date
6 on which an agency system risk assessment is
7 performed under subparagraph (A), providing
8 the assessment to—

9 “(i) the Director;

10 “(ii) the Director of the Cybersecurity
11 and Infrastructure Security Agency; and

12 “(iii) the National Cyber Director;

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

20 “(i) be completed considering the
21 agency system risk assessment performed
22 under subparagraph (A); and

23 “(ii) include a specific evaluation for
24 high value assets; and

1 “(G) not later than 30 days after com-
2 pleting the evaluation performed under sub-
3 paragraph (F), providing the evaluation and an
4 implementation plan for using additional cyber-
5 security procedures determined to be appro-
6 priate to—

7 “(i) the Director of the Cybersecurity
8 and Infrastructure Security Agency;

9 “(ii) the Director; and

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

11 (ii) in paragraph (2)—

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

17 (II) in subparagraph (B)—

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

21 “(i) standards”; and

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

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

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

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

9 (iii) in paragraph (3)—

10 (I) in subparagraph (B), by in-
11 serting “, in coordination with the Di-
12 rector of the Cybersecurity and Infra-
13 structure Security Agency,” after
14 “maintaining”;

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

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

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

21 “(F) implementing mechanisms for using
22 verification specifications, or alternate
23 verification specifications validated by the Di-
24 rector of the Cybersecurity and Infrastructure
25 Security Agency, in consultation with the Direc-

1 tor of the National Institute of Standards and
 2 Technology, to automatically verify the imple-
 3 mentation of standards of agency systems pro-
 4 mulgated under section 11331 of title 40 or any
 5 additional cybersecurity procedures, as applica-
 6 ble;” and

7 (iv) in paragraph (5), by inserting

8 “and the Director of the Cybersecurity and
 9 Infrastructure Security Agency” before
 10 “on the effectiveness”;

11 (B) in subsection (b)—

12 (i) by striking paragraph (1) and in-
 13 serting the following:

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

20 (ii) in paragraph (2)(D)—

21 (I) by redesignating clauses (iii)
 22 and (iv) as clauses (iv) and (v), re-
 23 spectively;

24 (II) by inserting after clause (ii)
 25 the following:

1 “(iii) binding operational directives
2 and emergency directives promulgated by
3 the Director of the Cybersecurity and In-
4 frastructure Security Agency under section
5 3553 of title 44;” and

6 (III) in clause (iv), as so redesign-
7 ated, by striking “as determined by
8 the agency; and” and inserting “as
9 determined by the agency—

10 “(I) in coordination with the Di-
11 rector of the Cybersecurity and Infra-
12 structure Security Agency; and

13 “(II) in consideration of—

14 “(aa) the agency risk assess-
15 ment performed under subsection
16 (a)(1)(A); and

17 “(bb) the determinations of
18 applying more stringent stand-
19 ards and additional cybersecurity
20 procedures pursuant to section
21 11331(e)(1) of title 40; and”;

22 (iii) in paragraph (5)—

23 (I) in subparagraph (A), by in-
24 serting “, including penetration test-

1 ing, as appropriate,” after “shall in-
2 clude testing”; and

3 (H) in subparagraph (C), by in-
4 serting “, verification specifications,”
5 after “with standards”;

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

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

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

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

24 “(8) a process for providing the verification of
25 the implementation of standards promulgated under

1 section 11331 of title 40 using verification specifica-
2 tions, automation, and machine-readable data, to the
3 Director and the Director of the Cybersecurity and
4 Infrastructure Security Agency;” and

5 (vii) in paragraph (9)(C), as so redes-
6 ignated—

7 (I) by striking clause (ii) and in-
8 serting the following:

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

13 (II) by redesignating clause (iii)
14 as clause (iv);

15 (III) by inserting after clause (ii)
16 the following:

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

20 (IV) in clause (iv), as so redesi-
21 gnated—

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

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

3 (cc) by striking subclause
4 (III); and

5 (dd) by redesignating sub-
6 clause (IV) as subclause (III);

7 (C) in subsection (c)—

8 (i) in paragraph (1)—

9 (I) in subparagraph (A)—

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

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

22 (II) by striking subparagraph (B)
23 and inserting the following:

24 “(B) INCIDENT REPORTING WAIVER.—

1 “(i) CERTIFICATION OF AGENCY IN-
2 FORMATION SHARING.—If the Director, in
3 consultation with the Director of the Cy-
4 bersecurity and Infrastructure Security
5 Agency, determines that an agency shares
6 any information relating to any incident
7 pursuant to section 3594(a), the Director
8 shall certify that the agency is in compli-
9 ance with that section.

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

22 “(iii) WAIVER.—The Director may
23 waive the reporting requirement with re-
24 spect to the information required to be in-

1 cluded in the report under subparagraph
2 (A)(ii) for a particular agency if—

3 “~~(I)~~ the Director has issued a
4 certification for the agency under
5 clause (i); and

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

9 “~~(iv)~~ ~~REVOCATION OF WAIVER OR~~
10 ~~CERTIFICATIONS.—~~

11 “~~(I)~~ ~~WAIVER.—~~If, at any time,
12 the Director determines that the Di-
13 rector of the Cybersecurity and Infra-
14 structure Security Agency cannot sub-
15 mit to Congress an annex for a par-
16 ticular agency under section
17 3597(e)(3)—

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

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

1 “(II) CERTIFICATIONS.—If, at
2 any time, the Director determines
3 that an agency has not provided to
4 the Director of the Cybersecurity and
5 Infrastructure Security Agency the to-
6 tality of incident information required
7 under section 3594(a)—

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

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

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

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

24 (iii) by inserting after paragraph (1)
25 the following:

1 “(2) BIENNIAL REPORT.—Not later than 180
2 days after the date on which an agency completes an
3 agency system risk assessment under subsection
4 (a)(1)(A) and not less frequently than every 2 years,
5 each agency shall submit to the Director, the Sec-
6 retary, the Committee on Homeland Security and
7 Governmental Affairs of the Senate, the Committee
8 on Oversight and Reform of the House of Represent-
9 atives, the Committee on Homeland Security of the
10 House of Representatives, the appropriate authoriza-
11 tion and appropriations committees of Congress, the
12 National Cyber Director, and the Comptroller Gen-
13 eral of the United States a report that—

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

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

23 “(C) summarizes the evaluations and im-
24 plementation plans described in subparagraphs
25 (F) and (G) of subsection (a)(1) and whether

1 those evaluations and implementation plans call
 2 for the use of additional cybersecurity proce-
 3 dures determined to be appropriate by the
 4 agency.

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

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

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

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

15 (4) in section 3555—

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

20 (B) by striking subsection (f) and inserting
 21 the following:

22 “(f) PROTECTION OF INFORMATION.—(1) Agencies
 23 and evaluators shall take appropriate steps to ensure the
 24 protection of information which, if disclosed, may ad-
 25 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).”;

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”;

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”;

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

4 “(h) BINDING OPERATIONAL DIRECTIVE.—If the Di-
5 rector of the Cybersecurity and Infrastructure Security
6 Agency issues a binding operational directive or an emer-
7 gency directive under section 3553, not later than 2 days
8 after the date on which the binding operational directive
9 requires an agency to take an action, each agency shall
10 provide to the appropriate notification entities the status
11 of the implementation of the binding operational directive
12 at the agency.

13 **“§ 3594. Government information sharing and inci-**
14 **dent response**

15 “(a) IN GENERAL.—

16 “(1) INCIDENT REPORTING.—The head of each
17 agency shall provide any information relating to any
18 incident, whether the information is obtained by the
19 Federal Government directly or indirectly, to the Cy-
20 bersecurity and Infrastructure Security Agency and
21 the Office of Management and Budget.

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

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 recipient 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 “(e) 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 “(e) 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 (e) 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 guidancee**

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 (e)(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 (e)(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 “(e) 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 (e);

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 (e)(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).”;

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 serting “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 (e) 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”;

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.”;

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

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”;

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 “(e) 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(e) 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 (e)
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(e) 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(e) 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 pro-
3 cesses 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(e)(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(e)(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 (e) 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(e) of the Cybersecurity~~
13 ~~Act of 2015 (6 U.S.C. 1522(e)), 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 H 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 (e).

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 “(e) 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(e)(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 ~~“(e) 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 disclosure
3 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 agency;
8 and

9 “(iv) the disclosure policy of the agency
10 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 reporter
20 should anticipate an acknowledgment
21 of receipt of the report by the agency;
22 and

23 “(D) include any other relevant information.
24

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 (e) 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 (e);

13 (2) submit to the appropriate congressional
14 committees a report on the results of the pilot pro-
15 gram established under subsection (e), 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 ecurity 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).

19 **SECTION 1. SHORT TITLE.**

20 *This Act may be cited as the “Federal Information Se-*
21 *curity Modernization Act of 2021”.*

22 **SEC. 2. TABLE OF CONTENTS.**

23 *The table of contents for this Act is as follows:*

Sec. 1. Short title.

Sec. 2. Table of contents.

Sec. 3. Definitions.

TITLE I—UPDATES TO FISMA

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

TITLE II—IMPROVING FEDERAL CYBERSECURITY

- Sec. 201. Mobile security standards.*
Sec. 202. Data and logging retention for incident response.
Sec. 203. CISA agency advisors.
Sec. 204. Federal penetration testing policy.
Sec. 205. Ongoing threat hunting program.
Sec. 206. Codifying vulnerability disclosure programs.
Sec. 207. Implementing presumption of compromise and least privilege principles.
Sec. 208. Automation reports.
Sec. 209. Extension of Federal acquisition security council.
Sec. 210. Council of the Inspectors General on Integrity and Efficiency dashboard.

TITLE III—RISK-BASED BUDGET MODEL

- Sec. 301. Definitions.*
Sec. 302. Establishment of risk-based budget model.

TITLE IV—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

- Sec. 401. Active cyber defensive study.*
Sec. 402. Security operations center as a service pilot.

1 **SEC. 3. DEFINITIONS.**

2 *In this Act, unless otherwise specified:*

3 (1) *ADDITIONAL CYBERSECURITY PROCEDURE.*—

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

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

1 (3) *APPROPRIATE CONGRESSIONAL COMMIT-*
2 *TEES.—The term “appropriate congressional commit-*
3 *tees” means—*

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

6 (B) *the Committee on Oversight and Reform*
7 *of the House of Representatives; and*

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

10 (4) *DIRECTOR.—The term “Director” means the*
11 *Director of the Office of Management and Budget.*

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

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

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

23 (8) *THREAT HUNTING.—The term “threat hunt-*
24 *ing” means proactively and iteratively searching for*

1 *threats to systems that evade detection by automated*
 2 *threat detection systems.*

3 **TITLE I—UPDATES TO FISMA**

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

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

7 (1) *in section 3504—*

8 (A) *in subsection (a)(1)(B)—*

9 (i) *by striking clause (v) and inserting*
 10 *the following:*

11 “(v) *confidentiality, disclosure, and sharing*
 12 *of information;*”;

13 (ii) *by redesignating clause (vi) as*
 14 *clause (vii); and*

15 (iii) *by inserting after clause (v) the*
 16 *following:*

17 “(vi) *in consultation with the National*
 18 *Cyber Director and the Director of the Cyberse-*
 19 *curity and Infrastructure Security Agency, secu-*
 20 *rity of information; and*”;

21 (B) *in subsection (g), by striking paragraph*
 22 (1) *and inserting the following:*

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

1 “(A) develop and oversee the implementa-
2 tion of policies, principles, standards, and guide-
3 lines on privacy, confidentiality, disclosure, and
4 sharing of the information; and

5 “(B) in consultation with the National
6 Cyber Director and the Director of the Cyberse-
7 curity and Infrastructure Security Agency, de-
8 velop and oversee policies, principles, standards,
9 and guidelines on security of the information;
10 and”;

11 (C) in subsection (h)(1)—

12 (i) in the matter preceding subpara-
13 graph (A)—

14 (I) by inserting “the Director of
15 the Cybersecurity and Infrastructure
16 Security Agency and the National
17 Cyber Director,” before “the Director”;
18 and

19 (II) by inserting a comma before
20 “and the Administrator”; and

21 (ii) in subparagraph (A), by inserting
22 “security and” after “information tech-
23 nology”;

24 (2) in section 3505—

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

3 (i) in subparagraph (B)—

4 (I) by inserting “the Director of
5 the Cybersecurity and Infrastructure
6 Security Agency, the National Cyber
7 Director, and” before “the Comptroller
8 General”; and

9 (II) by striking “and” at the end;

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

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

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

18 (B) by striking the second subsection des-
19 ignated as subsection (c);

20 (3) in section 3506—

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

23 (B) in subsection (h)(3), by inserting “secu-
24 rity,” after “efficiency,”; and

25 (4) in section 3513—

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

3 (B) by inserting after subsection (b) the fol-
4 lowing:

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

10 (b) *SUBCHAPTER II DEFINITIONS.*—

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

13 (A) by redesignating paragraphs (1), (2),
14 (3), (4), (5), (6), and (7) as paragraphs (2), (3),
15 (4), (5), (6), (9), and (11), respectively;

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

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

24 (C) by inserting after paragraph (6), as so
25 redesignated, the following:

1 “(7) *The term ‘high value asset’ means informa-*
2 *tion or an information system that the head of an*
3 *agency determines so critical to the agency that the*
4 *loss or corruption of the information or the loss of ac-*
5 *cess to the information system would have a serious*
6 *impact on the ability of the agency to perform the*
7 *mission of the agency or conduct business.*

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

11 *(D) by inserting after paragraph (9), as so*
12 *redesignated, the following:*

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

15 *“(A) is conducted on an information system*
16 *or a component of an information system; and*

17 *“(B) emulates an attack or other exploi-*
18 *tation capability of a potential adversary, typi-*
19 *cally under specific constraints, in order to iden-*
20 *tify any vulnerabilities of an information system*
21 *or a component of an information system that*
22 *could be exploited.”; and*

23 *(E) by inserting after paragraph (11), as so*
24 *redesignated, the following:*

1 “(12) *The term ‘shared service’ means a central-*
2 *ized business or mission capability that is provided to*
3 *multiple organizations within an agency or to mul-*
4 *tiple agencies.”.*

5 (2) *CONFORMING AMENDMENTS.—*

6 (A) *HOMELAND SECURITY ACT OF 2002.—*
7 *Section 1001(c)(1)(A) of the Homeland Security*
8 *Act of 2002 (6 U.S.C. 511(1)(A)) is amended by*
9 *striking “section 3552(b)(5)” and inserting “sec-*
10 *tion 3552(b)”.*

11 (B) *TITLE 10.—*

12 (i) *SECTION 2222.—Section 2222(i)(8)*
13 *of title 10, United States Code, is amended*
14 *by striking “section 3552(b)(6)(A)” and in-*
15 *serting “section 3552(b)(9)(A)”.*

16 (ii) *SECTION 2223.—Section 2223(c)(3)*
17 *of title 10, United States Code, is amended*
18 *by striking “section 3552(b)(6)” and insert-*
19 *ing “section 3552(b)”.*

20 (iii) *SECTION 2315.—Section 2315 of*
21 *title 10, United States Code, is amended by*
22 *striking “section 3552(b)(6)” and inserting*
23 *“section 3552(b)”.*

24 (iv) *SECTION 2339A.—Section*
25 *2339a(e)(5) of title 10, United States Code,*

1 is amended by striking “section 3552(b)(6)”
2 and inserting “section 3552(b)”.

3 (C) *HIGH-PERFORMANCE COMPUTING ACT*
4 *OF 1991*.—Section 207(a) of the *High-Perform-*
5 *ance Computing Act of 1991 (15 U.S.C. 5527(a))*
6 is amended by striking “section
7 3552(b)(6)(A)(i)” and inserting “section
8 3552(b)(9)(A)(i)”.

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

15 (E) *NATIONAL DEFENSE AUTHORIZATION*
16 *ACT FOR FISCAL YEAR 2013*.—Section
17 933(e)(1)(B) of the *National Defense Authoriza-*
18 *tion Act for Fiscal Year 2013 (10 U.S.C. 2224*
19 *note)* is amended by striking “section
20 3542(b)(2)” and inserting “section 3552(b)”.

21 (F) *IKE SKELTON NATIONAL DEFENSE AU-*
22 *THORIZATION ACT FOR FISCAL YEAR 2011*.—The
23 *Ike Skelton National Defense Authorization Act*
24 *for Fiscal Year 2011 (Public Law 111–383)* is
25 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 3542(b)(2)”
6 and inserting “section 3552(b)”;

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

10 (G) *E-GOVERNMENT ACT OF 2002*.—Section
11 301(c)(1)(A) of the *E-Government Act of 2002*
12 (44 U.S.C. 3501 note) is amended by striking
13 “section 3542(b)(2)” and inserting “section
14 3552(b)”.

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

19 (i) in subsection (a)(2), by striking
20 “section 3552(b)(5)” and inserting “section
21 3552(b)”;

22 (ii) in subsection (f)—

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

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

4 (c) *SUBCHAPTER II AMENDMENTS.*—Subchapter II of
5 chapter 35 of title 44, United States Code, is amended—

6 (1) in section 3551—

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

10 (B) by inserting after paragraph (2) the fol-
11 lowing:

12 “(3) recognize the role of the Cybersecurity and
13 Infrastructure Security Agency as the lead entity for
14 operational cybersecurity coordination across the Fed-
15 eral Government;”;

16 (C) in paragraph (5), as so redesignated, by
17 striking “diagnose and improve” and inserting
18 “integrate, deliver, diagnose, and improve”;

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

21 (E) in paragraph (7), as so redesignated, by
22 striking the period at the end and inserting a
23 semi colon; and

24 (F) by adding at the end the following:

1 “(8) recognize that each agency has specific mis-
2 sion requirements and, at times, unique cybersecurity
3 requirements to meet the mission of the agency;

4 “(9) recognize that each agency does not have the
5 same resources to secure agency systems, and an agen-
6 cy should not be expected to have the capability to se-
7 cure the systems of the agency from advanced adver-
8 saries alone; and

9 “(10) recognize that—

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

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

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

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

22 “(iii) the National Cyber Director is
23 responsible for developing the overall cyber-
24 security strategy of the United States and

1 *advising the President on matters relating*
2 *to cybersecurity.”;*

3 (2) *in section 3553—*

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

9 (B) *in subsection (a)—*

10 (i) *in paragraph (1), by inserting “in*
11 *coordination with the Director of the Cyber-*
12 *security and Infrastructure Security Agency*
13 *and the National Cyber Director,” before*
14 *“developing and overseeing”;*

15 (ii) *in paragraph (5)—*

16 (I) *by inserting “, in consultation*
17 *with the Director of the Cybersecurity*
18 *and Infrastructure Security Agency*
19 *and the National Cyber Director,” be-*
20 *fore “agency compliance”; and*

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

22 *and*

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

1 “(8) promoting, in consultation with the Direc-
2 tor of the Cybersecurity and Infrastructure Security
3 Agency and the Director of the National Institute of
4 Standards and Technology—

5 “(A) the use of automation to improve Fed-
6 eral cybersecurity and visibility with respect to
7 the implementation of Federal cybersecurity; and

8 “(B) the use of presumption of compromise
9 and least privilege principles to improve resil-
10 iency and timely response actions to incidents on
11 Federal systems.”;

12 (C) in subsection (b)—

13 (i) by striking the subsection heading
14 and inserting “CYBERSECURITY AND INFRA-
15 STRUCTURE SECURITY AGENCY”;

16 (ii) in the matter preceding paragraph
17 (1), by striking “The Secretary, in consulta-
18 tion with the Director” and inserting “The
19 Director of the Cybersecurity and Infra-
20 structure Security Agency, in consultation
21 with the Director and the National Cyber
22 Director”;

23 (iii) in paragraph (2)—

24 (I) in subparagraph (A), by in-
25 serting “and reporting requirements

1 *under subchapter IV of this title” after*
2 *“section 3556”; and*

3 (II) *in subparagraph (D), by*
4 *striking “the Director or Secretary”*
5 *and inserting “the Director of the Cy-*
6 *bersecurity and Infrastructure Security*
7 *Agency”;*

8 (iv) *in paragraph (5), by striking “co-*
9 *ordinating” and inserting “leading the co-*
10 *ordination of”;*

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

15 (vi) *in paragraph (9), by striking “as*
16 *the Director or the Secretary, in consulta-*
17 *tion with the Director,” and inserting “as*
18 *the Director of the Cybersecurity and Infra-*
19 *structure Security Agency”;*

20 (D) *in subsection (c)—*

21 (i) *in the matter preceding paragraph*
22 (1), *by striking “each year” and inserting*
23 *“each year during which agencies are re-*
24 *quired to submit reports under section*
25 *3554(c)”;*

1 (ii) by striking paragraph (1);

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

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

7 (v) by inserting after paragraph (3),
8 as so redesignated the following:

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

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

13 (E) by redesignating subsections (i), (j), (k),
14 and (l) as subsections (j), (k), (l), and (m) re-
15 spectively;

16 (F) by inserting after subsection (h) the fol-
17 lowing:

18 “(i) *FEDERAL RISK ASSESSMENTS*.—On an ongoing
19 and continuous basis, the Director of the Cybersecurity and
20 Infrastructure Security Agency shall perform assessments
21 of Federal risk posture using any available information on
22 the cybersecurity posture of agencies, and brief the Director
23 and National Cyber Director on the findings of those assess-
24 ments including—

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

3 “(2) any vulnerability information relating to
4 the systems of an agency that is known by the agency;

5 “(3) analysis of incident information under sec-
6 tion 3597;

7 “(4) evaluation of penetration testing performed
8 under section 3559A;

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

11 “(6) evaluation of agency threat hunting results;

12 “(7) evaluation of Federal and non-Federal
13 threat intelligence;

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

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

18 “(10) any other information the Director of the
19 Cybersecurity and Infrastructure Security Agency de-
20 termines relevant.”; and

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

22 (i) by striking “regarding the specific”
23 and inserting “that includes a summary
24 of—

25 “(1) the specific”;

1 (ii) in paragraph (1), as so designated,
2 by striking the period at the end and insert-
3 ing “; and” and

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

6 “(2) the trends identified in the Federal risk as-
7 sessment performed under subsection (i).”; and

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

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

19 (3) in section 3554—

20 (A) in subsection (a)—

21 (i) in paragraph (1)—

22 (I) by redesignating subpara-
23 graphs (A), (B), and (C) as subpara-
24 graphs (B), (C), and (D), respectively;

1 (II) by inserting before subpara-
2 graph (B), as so redesignated, the fol-
3 lowing:

4 “(A) on an ongoing and continuous basis,
5 performing agency system risk assessments
6 that—

7 “(i) identify and document the high
8 value assets of the agency using guidance
9 from the Director;

10 “(ii) evaluate the data assets inven-
11 toried under section 3511 for sensitivity to
12 compromises in confidentiality, integrity,
13 and availability;

14 “(iii) identify agency systems that
15 have access to or hold the data assets inven-
16 toried under section 3511;

17 “(iv) evaluate the threats facing agency
18 systems and data, including high value as-
19 sets, based on Federal and non-Federal
20 cyber threat intelligence products, where
21 available;

22 “(v) evaluate the vulnerability of agen-
23 cy systems and data, including high value
24 assets, including by analyzing—

1 “(I) the results of penetration test-
2 ing performed by the Department of
3 Homeland Security under section
4 3553(b)(9);

5 “(II) the results of penetration
6 testing performed under section 3559A;

7 “(III) information provided to the
8 agency through the vulnerability dis-
9 closure program of the agency under
10 section 3559B;

11 “(IV) incidents; and

12 “(V) any other vulnerability in-
13 formation relating to agency systems
14 that is known to the agency;

15 “(vi) assess the impacts of potential
16 agency incidents to agency systems, data,
17 and operations based on the evaluations de-
18 scribed in clauses (ii) and (iv) and the
19 agency systems identified under clause (iii);
20 and

21 “(vii) assess the consequences of poten-
22 tial incidents occurring on agency systems
23 that would impact systems at other agen-
24 cies, including due to interconnectivity be-
25 tween different agency systems or oper-

1 *ational reliance on the operations of the sys-*
2 *tem or data in the system;”;*

3 *(III) in subparagraph (B), as so*
4 *redesignated, in the matter preceding*
5 *clause (i), by striking “providing in-*
6 *formation” and inserting “using infor-*
7 *mation from the assessment conducted*
8 *under subparagraph (A), providing, in*
9 *coordination with the Director of the*
10 *Cybersecurity and Infrastructure Secu-*
11 *rity Agency, information”;*

12 *(IV) in subparagraph (C), as so*
13 *redesignated—*

14 *(aa) in clause (ii) by insert-*
15 *ing “binding” before “oper-*
16 *ational”; and*

17 *(bb) in clause (vi), by strik-*
18 *ing “and” at the end; and*

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

21 *“(E) providing an update on the ongoing*
22 *and continuous assessment performed under sub-*
23 *paragraph (A)—*

1 “(i) upon request, to the inspector gen-
2 eral of the agency or the Comptroller Gen-
3 eral of the United States; and

4 “(ii) on a periodic basis, as determined
5 by guidance issued by the Director but not
6 less frequently than annually, to—

7 “(I) the Director;

8 “(II) the Director of the Cyberse-
9 curity and Infrastructure Security
10 Agency; and

11 “(III) the National Cyber Direc-
12 tor;

13 “(F) in consultation with the Director of
14 the Cybersecurity and Infrastructure Security
15 Agency and not less frequently than once every
16 3 years, performing an evaluation of whether ad-
17 ditional cybersecurity procedures are appro-
18 priate for securing a system of, or under the su-
19 pervision of, the agency, which shall—

20 “(i) be completed considering the agen-
21 cy system risk assessment performed under
22 subparagraph (A); and

23 “(ii) include a specific evaluation for
24 high value assets;

1 “(G) not later than 30 days after com-
2 pleting the evaluation performed under subpara-
3 graph (F), providing the evaluation and an im-
4 plementation plan, if applicable, for using addi-
5 tional cybersecurity procedures determined to be
6 appropriate to—

7 “(i) the Director of the Cybersecurity
8 and Infrastructure Security Agency;

9 “(ii) the Director; and

10 “(iii) the National Cyber Director; and

11 “(H) if the head of the agency determines
12 there is need for additional cybersecurity proce-
13 dures, ensuring that those additional cybersecu-
14 rity procedures are reflected in the budget request
15 of the agency in accordance with the risk-based
16 cyber budget model developed pursuant to section
17 3553(a)(7);”;

18 (ii) in paragraph (2)—

19 (I) in subparagraph (A), by in-
20 serting “in accordance with the agency
21 system risk assessment performed
22 under paragraph (1)(A)” after “infor-
23 mation systems”;

24 (II) in subparagraph (B)—

1 (aa) by striking “in accord-
2 ance with standards” and insert-
3 ing “in accordance with—

4 “(i) standards”; and

5 (bb) by adding at the end the
6 following:

7 “(ii) the evaluation performed under
8 paragraph (1)(F); and

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

11 (III) in subparagraph (D), by in-
12 serting “, through the use of penetra-
13 tion testing, the vulnerability disclo-
14 sure program established under section
15 3559B, and other means,” after “peri-
16 odically”;

17 (iii) in paragraph (3)—

18 (I) in subparagraph (A)—

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

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

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

25 “(v) ensure that—

1 “(I) senior agency information se-
2 curity officers of component agencies
3 carry out responsibilities under this
4 subchapter, as directed by the senior
5 agency information security officer of
6 the agency or an equivalent official;
7 and

8 “(II) senior agency information
9 security officers of component agencies
10 report to—

11 “(aa) the senior information
12 security officer of the agency or
13 an equivalent official; and

14 “(bb) the Chief Information
15 Officer of the component agency
16 or an equivalent official;” and

17 (iv) in paragraph (5), by inserting
18 “and the Director of the Cybersecurity and
19 Infrastructure Security Agency” before “on
20 the effectiveness”;

21 (B) in subsection (b)—

22 (i) by striking paragraph (1) and in-
23 serting the following:

24 “(1) pursuant to subsection (a)(1)(A), per-
25 forming ongoing and continuous agency system risk

1 *assessments, which may include using guidelines and*
2 *automated tools consistent with standards and guide-*
3 *lines promulgated under section 11331 of title 40, as*
4 *applicable;”;*

5 *(ii) in paragraph (2)—*

6 *(I) by striking subparagraph (B)*

7 *and inserting the following:*

8 *“(B) comply with the risk-based cyber budg-*
9 *et model developed pursuant to section*
10 *3553(a)(7);”;* and

11 *(II) in subparagraph (D)—*

12 *(aa) by redesignating clauses*

13 *(iii) and (iv) as clauses (iv) and*

14 *(v), respectively;*

15 *(bb) by inserting after clause*

16 *(i) the following:*

17 *“(iii) binding operational directives*
18 *and emergency directives promulgated by*
19 *the Director of the Cybersecurity and Infra-*
20 *structure Security Agency under section*
21 *3553;”;* and

22 *(cc) in clause (iv), as so re-*

23 *designated, by striking “as deter-*

24 *mined by the agency; and” and*

1 inserting “as determined by the
2 agency, considering—

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

6 “(II) the determinations of apply-
7 ing more stringent standards and ad-
8 ditional cybersecurity procedures pur-
9 suant to section 11331(c)(1) of title 40;
10 and”;

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

14 (iv) in paragraph (6), by striking
15 “planning, implementing, evaluating, and
16 documenting” and inserting “planning and
17 implementing and, in consultation with the
18 Director of the Cybersecurity and Infra-
19 structure Security Agency, evaluating and
20 documenting”;

21 (v) by redesignating paragraphs (7)
22 and (8) as paragraphs (8) and (9), respec-
23 tively;

24 (vi) by inserting after paragraph (6)
25 the following:

1 “(7) a process for providing the status of every
2 remedial action and known system vulnerability to
3 the Director and the Director of the Cybersecurity
4 and Infrastructure Security Agency, using automa-
5 tion and machine-readable data to the greatest extent
6 practicable;” and

7 (vii) in paragraph (8)(C), as so redesi-
8 gnated—

9 (I) by striking clause (ii) and in-
10 sserting the following:

11 “(ii) notifying and consulting with the
12 Federal information security incident center
13 established under section 3556 pursuant to
14 the requirements of section 3594;”;

15 (II) by redesignating clause (iii)
16 as clause (iv);

17 (III) by inserting after clause (ii)
18 the following:

19 “(iii) performing the notifications and
20 other activities required under subchapter
21 IV of this title; and”;

22 (IV) in clause (iv), as so redesi-
23 gnated—

1 (aa) in subclause (I), by
2 striking “and relevant offices of
3 inspectors general”;

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

6 (cc) by striking subclause
7 (III); and

8 (dd) by redesignating sub-
9 clause (IV) as subclause (III);

10 (C) in subsection (c)—

11 (i) by redesignating paragraph (2) as
12 paragraph (5);

13 (ii) by striking paragraph (1) and in-
14 serting the following:

15 “(1) *BIANNUAL REPORT.*—Not later than 2 years
16 after the date of enactment of the Federal Information
17 Security Modernization Act of 2021 and not less fre-
18 quently than once every 2 years thereafter, using the
19 continuous and ongoing agency system risk assess-
20 ment under subsection (a)(1)(A), the head of each
21 agency shall submit to the Director, the Director of
22 the Cybersecurity and Infrastructure Security Agen-
23 cy, the Committee on Homeland Security and Gov-
24 ernmental Affairs of the Senate, the Committee on
25 Oversight and Reform of the House of Representa-

1 *tives, the Committee on Homeland Security of the*
2 *House of Representatives, the appropriate authoriza-*
3 *tion and appropriations committees of Congress, the*
4 *National Cyber Director, and the Comptroller General*
5 *of the United States a report that—*

6 *“(A) summarizes the agency system risk as-*
7 *essment performed under subsection (a)(1)(A);*

8 *“(B) evaluates the adequacy and effective-*
9 *ness of information security policies, procedures,*
10 *and practices of the agency to address the risks*
11 *identified in the agency system risk assessment*
12 *performed under subsection (a)(1)(A);*

13 *“(C) summarizes the evaluation and imple-*
14 *mentation plans described in subparagraphs (F)*
15 *and (G) of subsection (a)(1) and whether those*
16 *evaluation and implementation plans call for the*
17 *use of additional cybersecurity procedures deter-*
18 *mined to be appropriate by the agency; and*

19 *“(D) summarizes the status of remedial ac-*
20 *tions identified by inspector general of the agen-*
21 *cy, the Comptroller General of the United States,*
22 *and any other source determined appropriate by*
23 *the head of the agency.*

24 *“(2) UNCLASSIFIED REPORTS.—Each report sub-*
25 *mitted under paragraph (1)—*

1 “(A) shall be, to the greatest extent prac-
2 ticable, in an unclassified and otherwise uncon-
3 trolled form; and

4 “(B) may include a classified annex.

5 “(3) ACCESS TO INFORMATION.—The head of an
6 agency shall ensure that, to the greatest extent prac-
7 ticable, information is included in the unclassified
8 form of the report submitted by the agency under
9 paragraph (2)(A).

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

16 (iii) in paragraph (5), as so redesign-
17 ated, by inserting “including the reporting
18 procedures established under section
19 11315(d) of title 40 and subsection
20 (a)(3)(A)(v) of this section”; and

21 (D) in subsection (d)(1), in the matter pre-
22 ceding subparagraph (A), by inserting “and the
23 Director of the Cybersecurity and Infrastructure
24 Security Agency” after “the Director”; and

25 (4) in section 3555—

1 (A) in the section heading, by striking “**AN-**
2 **NUAL INDEPENDENT**” and inserting “**INDE-**
3 **PENDENT**”;

4 (B) in subsection (a)—

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

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

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

16 “(3) An evaluation under this section may include rec-
17 ommendations for improving the cybersecurity posture of
18 the agency.”;

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

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

24 (E) by striking subsection (f) and inserting
25 the following:

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

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

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

16 “(A) *specific information system incidents; or*

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

19 “(F) *in subsection (g)(2)—*

20 “(i) *by striking “this subsection shall”*
 21 *and inserting “this subsection—*

22 “(A) *shall”;*

23 “(ii) *in subparagraph (A), 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 “(B) identify any entity that performs an inde-
4 pendent evaluation under subsection (b).”; and

5 (G) by striking subsection (j) and inserting
6 the following:

7 “(j) GUIDANCE.—

8 “(1) IN GENERAL.—The Director, in consultation
9 with the Director of the Cybersecurity and Infrastruc-
10 ture Security Agency, the Chief Information Officers
11 Council, the Council of the Inspectors General on In-
12 tegrity and Efficiency, and other interested parties as
13 appropriate, shall ensure the development of guidance
14 for evaluating the effectiveness of an information se-
15 curity program and practices

16 “(2) PRIORITIES.—The guidance developed
17 under paragraph (1) shall prioritize the identification
18 of—

19 “(A) the most common threat patterns expe-
20 rienced by each agency;

21 “(B) the security controls that address the
22 threat patterns described in subparagraph (A);
23 and

24 “(C) any other security risks unique to the
25 networks of each agency.”; and

1 (5) *in section 3556(a)—*

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

6 (B) *in paragraph (4), by striking “3554(b)”*
 7 *and inserting “3554(a)(1)(A)”.*

8 (d) *CONFORMING AMENDMENTS.—*

9 (1) *TABLE OF SECTIONS.—The table of sections*
 10 *for chapter 35 of title 44, United States Code, is*
 11 *amended—*

12 (A) *by striking the item relating to section*
 13 *3553 and inserting the following:*

“3553. Authority and functions of the Director and the Director of the Cybersecu-
rity and Infrastructure Security Agency.”; and

14 (B) *by striking the item relating to section*
 15 *3555 and inserting the following:*

“3555. Independent evaluation.”.

16 (2) *OMB REPORTS.—Section 226(c) of the Cy-*
 17 *bersecurity Act of 2015 (6 U.S.C. 1524(c)) is amend-*
 18 *ed—*

19 (A) *in paragraph (1)(B), in the matter pre-*
 20 *ceding clause (i), by striking “annually there-*
 21 *after” and inserting “thereafter during the years*
 22 *during which a report is required to be sub-*

1 mitted under section 3553(c) of title 44, United
2 States Code”; and

3 (B) in paragraph (2)(B), in the matter pre-
4 ceding clause (i)—

5 (i) by striking “annually thereafter”
6 and inserting “thereafter during the years
7 during which a report is required to be sub-
8 mitted under section 3553(c) of title 44,
9 United States Code”; and

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

13 (3) NIST RESPONSIBILITIES.—Section
14 20(d)(3)(B) of the National Institute of Standards
15 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is
16 amended by striking “annual”.

17 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

18 (1) IN GENERAL.—Chapter 35 of title 44, United
19 States Code, is amended by adding at the end the fol-
20 lowing:

1 “SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT
2 RESPONSE

3 “§ 3591. *Definitions*

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

7 “(b) *ADDITIONAL DEFINITIONS.*—*As used in this sub-*
8 *chapter:*

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

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

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

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

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

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

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

23 “(G) *the Director;*

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

1 “(I) the National Cyber Director;

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

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

6 “(2) AWARDEE.—The term ‘awardee’—

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

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

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

14 “(A) a compromise of the security, confiden-
15 tiality, or integrity of data in electronic form
16 that results in unauthorized access to, or an ac-
17 quisition of, personal information; or

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

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

23 “(A) a prime contractor of an agency or a
24 subcontractor of a prime contractor of an agen-
25 cy; and

1 “(B) any person or business that collects or
2 maintains information, including personally
3 identifiable information, on behalf of an agency.

4 “(5) *FEDERAL INFORMATION*.—The term ‘Fed-
5 eral information’ means information created, col-
6 lected, processed, maintained, disseminated, disclosed,
7 or disposed of by or for the Federal Government in
8 any medium or form.

9 “(6) *FEDERAL INFORMATION SYSTEM*.—The term
10 ‘Federal information system’ means an information
11 system used or operated by an agency, a contractor,
12 or another organization on behalf of an agency.

13 “(7) *INTELLIGENCE COMMUNITY*.—The term ‘in-
14 telligence community’ has the meaning given the term
15 in section 3 of the National Security Act of 1947 (50
16 U.S.C. 3003).

17 “(8) *NATIONWIDE CONSUMER REPORTING AGEN-*
18 *CY*.—The term ‘nationwide consumer reporting agen-
19 cy’ means a consumer reporting agency described in
20 section 603(p) of the Fair Credit Reporting Act (15
21 U.S.C. 1681a(p)).

22 “(9) *VULNERABILITY DISCLOSURE*.—The term
23 ‘vulnerability disclosure’ means a vulnerability iden-
24 tified under section 3559B.

1 **“§ 3592. Notification of breach**

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

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

12 “(A) the nature and sensitivity of the per-
13 sonally identifiable information affected by the
14 breach;

15 “(B) the likelihood of access to and use of
16 the personally identifiable information affected
17 by the breach;

18 “(C) the type of breach; and

19 “(D) any other factors determined by the
20 Director; and

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

24 “(A) to the last known mailing address of
25 the individual; or

1 “(B) through an appropriate alternative
2 method of notification that the head of the agen-
3 cy or a designated senior-level individual of the
4 agency selects based on factors determined by the
5 Director.

6 “(b) CONTENTS OF NOTICE.—Each notice of a breach
7 provided to an individual under subsection (a)(2) shall in-
8 clude—

9 “(1) a brief description of the rationale for the
10 determination that notice should be provided under
11 subsection (a);

12 “(2) if possible, a description of the types of per-
13 sonally identifiable information affected by the
14 breach;

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

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

19 “(B) may include a telephone number or a
20 website;

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

23 “(5) any applicable educational materials relat-
24 ing to what individuals can do in response to a
25 breach that potentially affects their personally identi-

1 *fiable information, including relevant information to*
2 *contact Federal law enforcement agencies and each*
3 *nationwide consumer reporting agency; and*

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

7 *“(c) DELAY OF NOTIFICATION.—*

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

12 *“(A) impede a criminal investigation or a*
13 *national security activity;*

14 *“(B) reveal sensitive sources and methods;*

15 *“(C) cause damage to national security; or*

16 *“(D) hamper security remediation actions.*

17 *“(2) DOCUMENTATION.—*

18 *“(A) IN GENERAL.—Any delay under para-*
19 *graph (1) shall be reported in writing to the Di-*
20 *rector, the Attorney General, the Director of Na-*
21 *tional Intelligence, the Secretary of Homeland*
22 *Security, the Director of the Cybersecurity and*
23 *Infrastructure Security Agency, and the head of*
24 *the agency and the inspector general of the agen-*
25 *cy that experienced the breach.*

1 “(B) *CONTENTS.*—A report required under
2 subparagraph (A) shall include a written state-
3 ment from the entity that delayed the notifica-
4 tion explaining the need for the delay.

5 “(C) *FORM.*—The report required under
6 subparagraph (A) shall be unclassified but may
7 include a classified annex.

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

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

21 “(e) *EXEMPTION FROM NOTIFICATION.*—

22 “(1) *IN GENERAL.*—The head of an agency, in
23 consultation with the inspector general of the agency,
24 may request an exemption from the Director from
25 complying with the notification requirements under

1 subsection (a) if the information affected by the
2 breach is determined by an independent evaluation to
3 be unreadable, including, as appropriate, instances in
4 which the information is—

5 “(A) encrypted; and

6 “(B) determined by the Director of the Cy-
7 bersecurity and Infrastructure Security Agency
8 to be of sufficiently low risk of exposure.

9 “(2) APPROVAL.—The Director shall determine
10 whether to grant an exemption requested under para-
11 graph (1) in consultation with—

12 “(A) the Director of the Cybersecurity and
13 Infrastructure Security Agency; and

14 “(B) the Attorney General.

15 “(3) DOCUMENTATION.—Any exemption granted
16 by the Director under paragraph (1) shall be reported
17 in writing to the head of the agency and the inspector
18 general of the agency that experienced the breach and
19 the Director of the Cybersecurity and Infrastructure
20 Security Agency.

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

23 “(1) the Director from issuing guidance relating
24 to notifications or the head of an agency from noti-

1 *ifying individuals potentially affected by breaches that*
2 *are not determined to be major incidents; or*

3 *“(2) the Director from issuing guidance relating*
4 *to notifications of major incidents or the head of an*
5 *agency from providing more information than de-*
6 *scribed in subsection (b) when notifying individuals*
7 *potentially affected by breaches.*

8 **“§ 3593. Congressional and Executive Branch reports**

9 *“(a) INITIAL REPORT.—*

10 *“(1) IN GENERAL.—Not later than 72 hours after*
11 *an agency has a reasonable basis to conclude that a*
12 *major incident occurred, the head of the agency im-*
13 *pacted by the major incident shall submit to the ap-*
14 *propriate reporting entities a written report and, to*
15 *the extent practicable, provide a briefing to the Com-*
16 *mittee on Homeland Security and Governmental Af-*
17 *airs of the Senate, the Committee on Oversight and*
18 *Reform of the House of Representatives, the Com-*
19 *mittee on Homeland Security of the House of Rep-*
20 *resentatives, and the appropriate authorization and*
21 *appropriations committees of Congress, taking into*
22 *account—*

23 *“(A) the information known at the time of*
24 *the report;*

1 “(B) the sensitivity of the details associated
2 with the major incident; and

3 “(C) the classification level of the informa-
4 tion contained in the report.

5 “(2) CONTENTS.—A report required under para-
6 graph (1) shall include, in a manner that excludes or
7 otherwise reasonably protects personally identifiable
8 information and to the extent permitted by applicable
9 law, including privacy and statistical laws—

10 “(A) a summary of the information avail-
11 able about the major incident, including how the
12 major incident occurred, information indicating
13 that the major incident may be a breach, and in-
14 formation relating to the major incident as a
15 breach, based on information available to agency
16 officials as of the date on which the agency sub-
17 mits the report;

18 “(B) if applicable, a description and any
19 associated documentation of any circumstances
20 necessitating a delay in or exemption to notifica-
21 tion to individuals potentially affected by the
22 major incident under subsection (c) or (e) of sec-
23 tion 3592; and

24 “(C) if applicable, an assessment of the im-
25 pacts to the agency, the Federal Government, or

1 *the security of the United States, based on infor-*
2 *mation available to agency officials on the date*
3 *on which the agency submits the report.*

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

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

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

19 “(3) *the status of compliance of the affected in-*
20 *formation system with applicable security require-*
21 *ments at the time of the major incident;*

22 “(4) *an estimate of the number of individuals*
23 *potentially affected by the major incident based on in-*
24 *formation available to agency officials as of the date*
25 *on which the agency provides the update;*

1 “(5) an assessment of the risk of harm to indi-
2 viduals potentially affected by the major incident
3 based on information available to agency officials as
4 of the date on which the agency provides the update;

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

11 “(7) the detection, response, and remediation ac-
12 tions of the agency, including any support provided
13 by the Cybersecurity and Infrastructure Security
14 Agency under section 3594(d) and status updates on
15 the notification process described in section 3592(a),
16 including any delay or exemption described in sub-
17 section (c) or (e), respectively, of section 3592, if ap-
18 plicable.

19 “(c) *UPDATE REPORT*.—If the agency determines that
20 there is any significant change in the understanding of the
21 agency of the scope, scale, or consequence of a major inci-
22 dent for which an agency submitted a written report under
23 subsection (a), the agency shall provide an updated report
24 to the appropriate reporting entities that includes informa-
25 tion relating to the change in understanding.

1 “(d) *ANNUAL REPORT.*—Each agency shall submit as
2 part of the annual report required under section 3554(c)(1)
3 of this title a description of each major incident that oc-
4 curred during the 1-year period preceding the date on which
5 the report is submitted.

6 “(e) *DELAY AND EXEMPTION REPORT.*—

7 “(1) *IN GENERAL.*—The Director shall submit to
8 the appropriate notification entities an annual report
9 on all notification delays and exemptions granted
10 pursuant to subsections (c) and (d) of section 3592.

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

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

18 “(g) *THREAT BRIEFING.*—

19 “(1) *IN GENERAL.*—Not later than 7 days after
20 the date on which an agency has a reasonable basis
21 to conclude that a major incident occurred, the head
22 of the agency, jointly with the National Cyber Direc-
23 tor and any other Federal entity determined appro-
24 priate by the National Cyber Director, shall provide
25 a briefing to the congressional committees described in

1 subsection (a)(1) on the threat causing the major inci-
2 dent.

3 “(2) COMPONENTS.—The briefing required under
4 paragraph (1)—

5 “(A) shall, to the greatest extent practicable,
6 include an unclassified component; and

7 “(B) may include a classified component.

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

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

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

15 **“§3594. Government information sharing and inci-**
16 **dent response**

17 “(a) IN GENERAL.—

18 “(1) INCIDENT REPORTING.—The head of each
19 agency shall provide any information relating to any
20 incident, whether the information is obtained by the
21 Federal Government directly or indirectly, to the Cy-
22 bersecurity and Infrastructure Security Agency and
23 the Office of Management and Budget.

1 “(2) *CONTENTS.*—A provision of information re-
2 *lating to an incident made by the head of an agency*
3 *under paragraph (1) shall—*

4 “(A) *include detailed information about the*
5 *safeguards that were in place when the incident*
6 *occurred;*

7 “(B) *whether the agency implemented the*
8 *safeguards described in subparagraph (A) cor-*
9 *rectly;*

10 “(C) *in order to protect against a similar*
11 *incident, identify—*

12 “(i) *how the safeguards described in*
13 *subparagraph (A) should be implemented*
14 *differently; and*

15 “(ii) *additional necessary safeguards;*
16 *and*

17 “(D) *include information to aid in incident*
18 *response, such as—*

19 “(i) *a description of the affected sys-*
20 *tems or networks;*

21 “(ii) *the estimated dates of when the*
22 *incident occurred; and*

23 “(iii) *information that could reason-*
24 *ably help identify the party that conducted*
25 *the incident.*

1 “(3) *INFORMATION SHARING.*—*To the greatest*
2 *extent practicable, the Director of the Cybersecurity*
3 *and Infrastructure Security Agency shall share infor-*
4 *mation relating to an incident with any agencies that*
5 *may be impacted by the incident.*

6 “(4) *NATIONAL SECURITY SYSTEMS.*—*Each agen-*
7 *cy operating or exercising control of a national secu-*
8 *rity system shall share information about incidents*
9 *with the Director of the Cybersecurity and Infrastruc-*
10 *ture Security Agency to the extent consistent with*
11 *standards and guidelines for national security sys-*
12 *tems issued in accordance with law and as directed*
13 *by the President.*

14 “(b) *COMPLIANCE.*—*The information provided under*
15 *subsection (a) shall take into account the level of classifica-*
16 *tion of the information and any information sharing limi-*
17 *tations and protections, such as limitations and protections*
18 *relating to law enforcement, national security, privacy, sta-*
19 *tistical confidentiality, or other factors determined by the*
20 *Director*

21 “(c) *INCIDENT RESPONSE.*—*Each agency that has a*
22 *reasonable basis to conclude that a major incident occurred*
23 *involving Federal information in electronic medium or*
24 *form, as defined by the Director and not involving a na-*
25 *tional security system, regardless of delays from notifica-*

1 *tion granted for a major incident, shall coordinate with the*
 2 *Cybersecurity and Infrastructure Security Agency regard-*
 3 *ing—*

4 “(1) *incident response and recovery; and*

5 “(2) *recommendations for mitigating future inci-*
 6 *dents.*

7 **“§3595. Responsibilities of contractors and awardees**

8 “(a) *NOTIFICATION.—*

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

16 “(A) *an incident or breach has occurred*
 17 *with respect to Federal information collected,*
 18 *used, or maintained by the contractor or award-*
 19 *ee in connection with the contract, grant, or co-*
 20 *operative agreement of the contractor or awardee;*

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

1 “(C) *the contractor or awardee has received*
2 *information from the agency that the contractor*
3 *or awardee is not authorized to receive in con-*
4 *nection with the contract, grant, or cooperative*
5 *agreement of the contractor or awardee.*

6 “(2) *PROCEDURES.—*

7 “(A) *MAJOR INCIDENT.—Following a report*
8 *of a breach or major incident by a contractor or*
9 *awardee under paragraph (1), the agency, in*
10 *consultation with the contractor or awardee,*
11 *shall carry out the requirements under sections*
12 *3592, 3593, and 3594 with respect to the major*
13 *incident.*

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

20 “(b) *EFFECTIVE DATE.—This section shall apply on*
21 *and after the date that is 1 year after the date of enactment*
22 *of the Federal Information Security Modernization Act of*
23 *2021.*

1 **“§ 3596. Training**

2 “(a) *COVERED INDIVIDUAL DEFINED.*—*In this section,*
3 *the term ‘covered individual’ means an individual who ob-*
4 *tains access to Federal information or Federal information*
5 *systems because of the status of the individual as an em-*
6 *ployee, contractor, awardee, volunteer, or intern of an agen-*
7 *cy.*

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

11 “(1) *the internal process of the agency for report-*
12 *ing an incident; and*

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

18 “(c) *INCLUSION IN ANNUAL TRAINING.*—*The training*
19 *developed under subsection (b) may be included as part of*
20 *an annual privacy or security awareness training of an*
21 *agency.*

22 **“§ 3597. Analysis and report on Federal incidents**

23 “(a) *ANALYSIS OF FEDERAL INCIDENTS.*—

24 “(1) *QUANTITATIVE AND QUALITATIVE ANAL-*
25 *YSES.*—*The Director of the Cybersecurity and Infra-*
26 *structure Security Agency shall develop, in consulta-*

1 *tion with the Director and the National Cyber Direc-*
2 *tor, and perform continuous monitoring and quan-*
3 *titative and qualitative analyses of incidents at agen-*
4 *cies, including major incidents, including—*

5 *“(A) the causes of incidents, including—*

6 *“(i) attacker tactics, techniques, and*
7 *procedures; and*

8 *“(ii) system vulnerabilities, including*
9 *zero days, unpatched systems, and informa-*
10 *tion system misconfigurations;*

11 *“(B) the scope and scale of incidents at*
12 *agencies;*

13 *“(C) cross Federal Government root causes*
14 *of incidents at agencies;*

15 *“(D) agency incident response, recovery,*
16 *and remediation actions and the effectiveness of*
17 *those actions, as applicable; and*

18 *“(E) lessons learned and recommendations*
19 *in responding to, recovering from, remediating,*
20 *and mitigating future incidents.*

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

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

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

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

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

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

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

14 “(ii) *to the greatest extent practicable,*
15 *in machine-readable formats in order to en-*
16 *able automated intake and use by agencies.*

17 “(b) *ANNUAL REPORT ON FEDERAL INCIDENTS.*—*Not*
18 *later than 2 years after the date of enactment of this section,*
19 *and not less frequently than annually thereafter, the Direc-*
20 *tor of the Cybersecurity and Infrastructure Security Agen-*
21 *cy, in consultation with the Director and other Federal*
22 *agencies as appropriate, shall submit to the appropriate no-*
23 *tification entities a report that includes—*

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

4 “(2) the quantitative and qualitative analyses of
5 incidents developed under subsection (a)(1), including
6 specific analysis of breaches, on an agency-by-agency
7 basis and comprehensively across the Federal Govern-
8 ment; and

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

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

11 and

12 “(B) the total number of compromises of the
13 agency.

14 “(c) *PUBLICATION*.—A version of each report sub-
15 mitted under subsection (b) shall be made publicly available
16 on the website of the Cybersecurity and Infrastructure Secu-
17 rity Agency during the year in which the report is sub-
18 mitted.

19 “(d) *INFORMATION PROVIDED BY AGENCIES*.—

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

24 “(2) *NONCOMPLIANCE REPORTS*.—

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

11 “(i) data for the incident; and

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

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

20 “(3) *NATIONAL SECURITY SYSTEM REPORTS.*—

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

1 *tent that the submission is consistent with stand-*
2 *ards and guidelines for national security systems*
3 *issued in accordance with law and as directed by*
4 *the President to—*

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

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

9 *“(iii) the Committee on Homeland Se-*
10 *curity and Governmental Affairs of the Sen-*
11 *ate;*

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

14 *“(v) the Committee on Armed Services*
15 *of the Senate;*

16 *“(vi) the Committee on Oversight and*
17 *Reform of the House of Representatives;*

18 *“(vii) the Committee on Homeland Se-*
19 *curity of the House of Representatives;*

20 *“(viii) the Permanent Select Com-*
21 *mittee on Intelligence of the House of Rep-*
22 *resentatives; and*

23 *“(ix) the Committee on Armed Services*
24 *of the House of Representatives.*

1 “(B) *CLASSIFIED FORM.*—A report required
2 under subparagraph (A) may be submitted in a
3 classified form.

4 “(e) *REQUIREMENT FOR COMPILING INFORMATION.*—
5 *In publishing the public report required under subsection*
6 *(c), the Director of the Cybersecurity and Infrastructure Se-*
7 *curity Agency shall sufficiently compile information such*
8 *that no specific incident of an agency can be identified, ex-*
9 *cept with the concurrence of the Director of the Office of*
10 *Management and Budget and in consultation with the im-*
11 *pacted agency.*

12 **“§ 3598. Major incident definition**

13 “(a) *IN GENERAL.*—Not later than 180 days after the
14 *date of enactment of the Federal Information Security Mod-*
15 *ernization Act of 2021, the Director, in coordination with*
16 *the Director of the Cybersecurity and Infrastructure Secu-*
17 *rity Agency and the National Cyber Director, shall develop*
18 *and promulgate guidance on the definition of the term*
19 *‘major incident’ for the purposes of subchapter II and this*
20 *subchapter.*

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

24 “(1) *include, with respect to any information*
25 *collected or maintained by or on behalf of an agency*

1 *or an information system used or operated by an*
2 *agency or by a contractor of an agency or another or-*
3 *ganization on behalf of an agency—*

4 *“(A) any incident the head of the agency*
5 *determines is likely to have an impact on—*

6 *“(i) the national security, homeland se-*
7 *curity, or economic security of the United*
8 *States; or*

9 *“(ii) the civil liberties or public health*
10 *and safety of the people of the United*
11 *States;*

12 *“(B) any incident the head of the agency*
13 *determines likely to result in an inability for the*
14 *agency, a component of the agency, or the Fed-*
15 *eral Government, to provide 1 or more critical*
16 *services;*

17 *“(C) any incident that the head of an agen-*
18 *cy, in consultation with a senior privacy officer*
19 *of the agency, determines is likely to have a sig-*
20 *nificant privacy impact on 1 or more indi-*
21 *vidual;*

22 *“(D) any incident that the head of the agen-*
23 *cy, in consultation with a senior privacy official*
24 *of the agency, determines is likely to have a sub-*

1 *stantial privacy impact on a significant number*
2 *of individuals;*

3 “(E) *any incident the head of the agency*
4 *determines impacts the operations of a high*
5 *value asset owned or operated by the agency;*

6 “(F) *any incident involving the exposure of*
7 *sensitive agency information to a foreign entity,*
8 *such as the communications of the head of the*
9 *agency, the head of a component of the agency,*
10 *or the direct reports of the head of the agency or*
11 *the head of a component of the agency; and*

12 “(G) *any other type of incident determined*
13 *appropriate by the Director;*

14 “(2) *stipulate that the National Cyber Director*
15 *shall declare a major incident at each agency im-*
16 *pacted by an incident if the Director of the Cyberse-*
17 *curity and Infrastructure Security Agency determines*
18 *that an incident—*

19 “(A) *occurs at not less than 2 agencies; and*

20 “(B) *is enabled by—*

21 “(i) *a common technical root cause,*
22 *such as a supply chain compromise, a com-*
23 *mon software or hardware vulnerability; or*

24 “(ii) *the related activities of a common*
25 *threat actor; and*

1 “(3) stipulate that, in determining whether an
2 incident constitutes a major incident because that in-
3 cident—

4 “(A) is any incident described in para-
5 graph (1), the head of an agency shall consult
6 with the Director of the Cybersecurity and Infra-
7 structure Security Agency;

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

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

14 “(i) the Privacy and Civil Liberties
15 Oversight Board; and

16 “(ii) the Executive Director of the Fed-
17 eral Trade Commission.

18 “(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In de-
19 termining what constitutes a significant number of individ-
20 uals under subsection (b)(1)(D), the Director—

21 “(1) may determine a threshold for a minimum
22 number of individuals that constitutes a significant
23 amount; and

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

1 “(d) *EVALUATION AND UPDATES.*—Not later than 2
 2 years after the date of enactment of the Federal Information
 3 Security Modernization Act of 2021, and not less frequently
 4 than every 2 years thereafter, the Director shall submit to
 5 the Committee on Homeland Security and Governmental
 6 Affairs of the Senate and the Committee on Oversight and
 7 Reform of the House of Representatives an evaluation,
 8 which shall include—

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

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

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

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

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification of breach.

“3593. Congressional and Executive Branch reports.

“3594. Government information sharing and incident response.

“3595. Responsibilities of contractors and awardees.

“3596. Training.

“3597. Analysis and report on Federal incidents.

“3598. Major incident definition.”.

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

20 (a) *INFORMATION TECHNOLOGY MODERNIZATION CEN-*
 21 *TERS OF EXCELLENCE PROGRAM ACT.*—Section

1 *2(c)(4)(A)(ii) of the Information Technology Modernization*
2 *Centers of Excellence Program Act (40 U.S.C. 11301 note)*
3 *is amended by striking the period at the end and inserting*
4 *“, which shall be provided in coordination with the Director*
5 *of the Cybersecurity and Infrastructure Security Agency.”.*

6 *(b) MODERNIZING GOVERNMENT TECHNOLOGY.—Sub-*
7 *title G of title X of Division A of the National Defense Au-*
8 *thorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note)*
9 *is amended—*

10 *(1) in section 1077(b)—*

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

14 *(B) in paragraph (7)—*

15 *(i) in the paragraph heading, by strik-*
16 *ing “CIO” and inserting “CIO”;*

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

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

21 *(iii) in subparagraph (A), as so des-*
22 *ignated, by striking “under section*
23 *1094(b)(1)” and inserting “by the Direc-*
24 *tor”;* and

25 *(iv) by adding at the end the following:*

1 “(B) *CONSULTATION.*—*In using funds*
 2 *under paragraph (3)(A), the Chief Information*
 3 *Officer of the covered agency shall consult with*
 4 *the necessary stakeholders to ensure the project*
 5 *appropriately addresses cybersecurity risks, in-*
 6 *cluding the Director of the Cybersecurity and In-*
 7 *frastructure Security Agency, as appropriate.”;*
 8 *and*
 9 *(2) in section 1078—*

10 *(A) by striking subsection (a) and inserting*
 11 *the following:*

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

13 “(1) *AGENCY.*—*The term ‘agency’ has the mean-*
 14 *ing given the term in section 551 of title 5, United*
 15 *States Code.*

16 “(2) *HIGH VALUE ASSET.*—*The term ‘high value*
 17 *asset’ has the meaning given the term in section 3552*
 18 *of title 44, United States Code.”;*

19 *(B) in subsection (b), by adding at the end*
 20 *the following:*

21 “(8) *PROPOSAL EVALUATION.*—*The Director*
 22 *shall—*

23 “(A) *give consideration for the use of*
 24 *amounts in the Fund to improve the security of*
 25 *high value assets; and*

1 “(B) require that any proposal for the use
2 of amounts in the Fund includes a cybersecurity
3 plan, including a supply chain risk management
4 plan, to be reviewed by the member of the Tech-
5 nology Modernization Board described in sub-
6 section (c)(5)(C).”; and

7 (C) in subsection (c)—

8 (i) in paragraph (2)(A)(i), by insert-
9 ing “, including a consideration of the im-
10 pact on high value assets” after “oper-
11 ational risks”;

12 (ii) in paragraph (5)—

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

15 (II) in subparagraph (B), by
16 striking the period at the end and in-
17 serting “and”; and

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

20 “(C) a senior official from the Cybersecurity
21 and Infrastructure Security Agency of the De-
22 partment of Homeland Security, appointed by
23 the Director.”; and

24 (iii) in paragraph (6)(A), by striking
25 “shall be—” and all that follows through “4

1 *employees” and inserting “shall be 4 em-*
2 *ployees”.*

3 *(c) SUBCHAPTER I.—Subchapter I of subtitle III of*
4 *title 40, United States Code, is amended—*

5 *(1) in section 11302—*

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

12 *(B) in subsection (c)—*

13 *(i) in paragraph (3)—*

14 *(I) in subparagraph (A)—*

15 *(aa) by striking “including*
16 *data” and inserting “which*
17 *shall—*

18 *“(i) include data”;*

19 *(bb) in clause (i), as so des-*
20 *ignated, by striking “, and per-*
21 *formance” and inserting “secu-*
22 *rity, and performance; and”;* and

23 *(cc) by adding at the end the*
24 *following:*

1 “(ii) specifically denote cybersecurity
2 funding under the risk-based cyber budget
3 model developed pursuant to section
4 3553(a)(7) of title 44.”; and

5 (II) in subparagraph (B), adding
6 at the end the following:

7 “(iii) The Director shall provide to the
8 National Cyber Director any cybersecurity
9 funding information described in subpara-
10 graph (A)(ii) that is provided to the Direc-
11 tor under clause (i) of this subparagraph.”;
12 and

13 (ii) in paragraph (4)(B), in the matter
14 preceding clause (i), by inserting “not later
15 than 30 days after the date on which the re-
16 view under subparagraph (A) is completed,”
17 before “the Administrator”;

18 (C) in subsection (f)—

19 (i) by striking “heads of executive
20 agencies to develop” and inserting “heads of
21 executive agencies to—

22 “(1) develop”;

23 (ii) in paragraph (1), as so designated,
24 by striking the period at the end and insert-
25 ing “; and”; and

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

3 “(2) consult with the Director of the Cybersecu-
4 rity and Infrastructure Security Agency for the devel-
5 opment and use of supply chain security best prac-
6 tices.”; and

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

10 (2) in section 11303(b)—

11 (A) in paragraph (2)(B)—

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

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

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

18 “(iii) whether the function should be
19 performed by a shared service offered by an-
20 other executive agency;”; and

21 (B) in paragraph (5)(B)(i), by inserting “,
22 while taking into account the risk-based cyber
23 budget model developed pursuant to section
24 3553(a)(7) of title 44” after “title 31”.

1 (d) *SUBCHAPTER II.*—Subchapter II of subtitle III of
2 *title 40, United States Code, is amended—*

3 (1) *in section 11312(a), by inserting “, including*
4 *security risks” after “managing the risks”;*

5 (2) *in section 11313(1), by striking “efficiency*
6 *and effectiveness” and inserting “efficiency, security,*
7 *and effectiveness”;*

8 (3) *in section 11315, by adding at the end the*
9 *following:*

10 “*(d) COMPONENT AGENCY CHIEF INFORMATION OFFI-*
11 *CERS.—The Chief Information Officer or an equivalent offi-*
12 *cial of a component agency shall report to—*

13 “*(1) the Chief Information Officer designated*
14 *under section 3506(a)(2) of title 44 or an equivalent*
15 *official of the agency of which the component agency*
16 *is a component; and*

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

18 “*(4) in section 11317, by inserting “security,” be-*
19 *fore “or schedule”; and*

20 “*(5) in section 11319(b)(1), in the paragraph*
21 *heading, by striking “CIOS” and inserting “CHIEF*
22 *INFORMATION OFFICERS”.*

23 (e) *SUBCHAPTER III.*—Section 11331 of title 40,
24 *United States Code, is amended—*

1 (1) *in subsection (a), by striking “section*
2 *3532(b)(1)” and inserting “section 3552(b)”;*

3 (2) *in subsection (b)(1)(A)—*

4 (A) *by striking “in consultation” and in-*
5 *serting “in coordination”;* and

6 (B) *by striking “the Secretary of Homeland*
7 *Security” and inserting “the Director of the Cy-*
8 *bersecurity and Infrastructure Security Agency”;*

9 (3) *by striking subsection (c) and inserting the*
10 *following:*

11 “(c) *APPLICATION OF MORE STRINGENT STAND-*
12 *ARDS.—*

13 “(1) *IN GENERAL.—The head of an agency*
14 *shall—*

15 “(A) *evaluate, in consultation with the sen-*
16 *ior agency information security officers, the need*
17 *to employ standards for cost-effective, risk-based*
18 *information security for all systems, operations,*
19 *and assets within or under the supervision of the*
20 *agency that are more stringent than the stand-*
21 *ards promulgated by the Director under this sec-*
22 *tion, if such standards contain, at a minimum,*
23 *the provisions of those applicable standards*
24 *made compulsory and binding by the Director;*
25 *and*

1 “(B) to the greatest extent practicable and
2 if the head of the agency determines that the
3 standards described in subparagraph (A) are
4 necessary, employ those standards.

5 “(2) *EVALUATION OF MORE STRINGENT STAND-*
6 *ARDS.—In evaluating the need to employ more strin-*
7 *gent standards under paragraph (1), the head of an*
8 *agency shall consider available risk information, such*
9 *as—*

10 “(A) the status of cybersecurity remedial ac-
11 tions of the agency;

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

14 “(C) incident information of the agency;

15 “(D) information from—

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

18 “(ii) information from the vulner-
19 ability disclosure program established under
20 section 3559B of title 44;

21 “(E) agency threat hunting results under
22 section 205 of the Federal Information Security
23 Modernization Act of 2021;

24 “(F) Federal and non-Federal threat intel-
25 ligence;

1 “(G) data on compliance with standards
2 issued under this section;

3 “(H) agency system risk assessments per-
4 formed under section 3554(a)(1)(A) of title 44;
5 and

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

8 (4) in subsection (d)(2)—

9 (A) in the paragraph heading, by striking
10 “NOTICE AND COMMENT” and inserting “CON-
11 SULTATION, NOTICE, AND COMMENT”;

12 (B) by inserting “promulgate,” before “sig-
13 nificantly modify”; and

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

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

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

1 *General of the United States, and the Council of*
2 *the Inspectors General on Integrity and Effi-*
3 *ciency;*

4 “(C) *considering the Federal risk assess-*
5 *ments performed under section 3553(i) of title*
6 *44; and*

7 “(D) *considering the extent to which the*
8 *proposed standard reduces risk relative to the*
9 *cost of implementation of the standard.”; and*
10 *(5) by adding at the end the following:*

11 “(e) *REVIEW OF OFFICE OF MANAGEMENT AND BUDG-*
12 *ET GUIDANCE AND POLICY.—*

13 “(1) *CONDUCT OF REVIEW.—*

14 “(A) *IN GENERAL.—Not less frequently than*
15 *once every 3 years, the Director of the Office of*
16 *Management and Budget, in consultation with*
17 *the Chief Information Officers Council, the Di-*
18 *rector of the Cybersecurity and Infrastructure*
19 *Security Agency, the National Cyber Director,*
20 *the Comptroller General of the United States,*
21 *and the Council of the Inspectors General on In-*
22 *tegrity and Efficiency shall review the efficacy of*
23 *the guidance and policy promulgated by the Di-*
24 *rector in reducing cybersecurity risks, including*
25 *an assessment of the requirements for agencies to*

1 *report information to the Director, and deter-*
2 *mine whether any changes to that guidance or*
3 *policy is appropriate.*

4 “(B) *FEDERAL RISK ASSESSMENTS.*—*In*
5 *conducting the review described in subparagraph*
6 *(A), the Director shall consider the Federal risk*
7 *assessments performed under section 3553(i) of*
8 *title 44.*

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

15 “(3) *PUBLIC REPORT.*—*Not later than 30 days*
16 *after the date on which a review is completed under*
17 *paragraph (1), the Director of the Office of Manage-*
18 *ment and Budget shall make publicly available a re-*
19 *port that includes—*

20 “(A) *an overview of the guidance and policy*
21 *promulgated under this section that is currently*
22 *in effect;*

23 “(B) *the cybersecurity risk mitigation, or*
24 *other cybersecurity benefit, offered by each guid-*

1 *ance or policy document described in subpara-*
2 *graph (A); and*

3 *“(C) a summary of the guidance or policy*
4 *to which changes were determined appropriate*
5 *during the review and what the changes are an-*
6 *ticipated to include.*

7 *“(4) CONGRESSIONAL BRIEFING.—Not later than*
8 *30 days after the date on which a review is completed*
9 *under paragraph (1), the Director shall provide to the*
10 *Committee on Homeland Security and Governmental*
11 *Affairs of the Senate and the Committee on Oversight*
12 *and Reform of the House of Representatives a briefing*
13 *on the review.*

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

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

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

5 (1) *IN GENERAL.—Not later than 180 days after*
6 *the date of enactment of this Act, the Director of the*
7 *Cybersecurity and Infrastructure Security Agency*
8 *shall—*

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

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

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

20 (B) *provide to the appropriate congressional*
21 *committees a briefing on the plan developed*
22 *under subparagraph (A).*

23 (2) *BRIEFING.—Not later than 1 year after the*
24 *date of enactment of this Act, the Director of the Cy-*
25 *bersecurity and Infrastructure Security Agency shall*

1 provide to the appropriate congressional committees a
2 briefing on—

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

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

8 (b) *RESPONSIBILITIES OF THE DIRECTOR OF THE OF-*
9 *FICE OF MANAGEMENT AND BUDGET.*—

10 (1) *FISMA.*—Section 2 of the *Federal Informa-*
11 *tion Security Modernization Act of 2014 (44 U.S.C.*
12 *3554 note)* is amended—

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

14 (B) by redesignating subsections (c) through
15 (f) as subsections (b) through (e), respectively.

16 (2) *INCIDENT DATA SHARING.*—

17 (A) *IN GENERAL.*—The Director shall de-
18 velop guidance, to be updated not less frequently
19 than once every 2 years, on the content, timeli-
20 ness, and format of the information provided by
21 agencies under section 3594(a) of title 44, United
22 States Code, as added by this Act.

23 (B) *REQUIREMENTS.*—The guidance devel-
24 oped under subparagraph (A) shall—

- 1 (i) *prioritize the availability of data*
2 *necessary to understand and analyze—*
- 3 (I) *the causes of incidents;*
4 (II) *the scope and scale of inci-*
5 *dents within the environments and sys-*
6 *tems of an agency;*
7 (III) *a root cause analysis of inci-*
8 *dents that—*
- 9 (aa) *are common across the*
10 *Federal Government; or*
- 11 (bb) *have a Government-wide*
12 *impact;*
- 13 (IV) *agency response, recovery,*
14 *and remediation actions and the effec-*
15 *tiveness of those actions; and*
- 16 (V) *the impact of incidents;*
- 17 (ii) *enable the efficient development*
18 *of—*
- 19 (I) *lessons learned and rec-*
20 *ommendations in responding to, recov-*
21 *ering from, remediating, and miti-*
22 *gating future incidents; and*
- 23 (II) *the report on Federal inci-*
24 *dents required under section 3597(b) of*

1 *title 44, United States Code, as added*
2 *by this Act;*

3 *(iii) include requirements for the time-*
4 *liness of data production; and*

5 *(iv) include requirements for using au-*
6 *tomation and machine-readable data for*
7 *data sharing and availability.*

8 *(3) GUIDANCE ON RESPONDING TO INFORMATION*
9 *REQUESTS.—Not later than 1 year after the date of*
10 *enactment of this Act, the Director shall develop guid-*
11 *ance for agencies to implement the requirement under*
12 *section 3594(c) of title 44, United States Code, as*
13 *added by this Act, to provide information to other*
14 *agencies experiencing incidents.*

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

25 *(5) CONTRACTOR AND AWARDEE GUIDANCE.—*

1 (A) *IN GENERAL.*—Not later than 1 year
2 after the date of enactment of this Act, the Direc-
3 tor, in coordination with the Secretary of Home-
4 land Security, the Secretary of Defense, the Ad-
5 ministrator of General Services, and the heads of
6 other agencies determined appropriate by the Di-
7 rector, shall issue guidance to Federal agencies
8 on how to deconflict, to the greatest extent prac-
9 ticable, existing regulations, policies, and proce-
10 dures relating to the responsibilities of contrac-
11 tors and awardees established under section 3595
12 of title 44, United States Code, as added by this
13 Act.

14 (B) *EXISTING PROCESSES.*—To the greatest
15 extent practicable, the guidance issued under
16 subparagraph (A) shall allow contractors and
17 awardees to use existing processes for notifying
18 Federal agencies of incidents involving informa-
19 tion of the Federal Government.

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

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

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

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

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

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

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

19 Not later than 1 year after the date of enactment of
 20 this Act, the Director, in coordination with the Director of
 21 the Cybersecurity and Infrastructure Security Agency, shall
 22 issue guidance for agencies on—

23 (1) performing the ongoing and continuous agen-
 24 cy system risk assessment required under section

1 *3554(a)(1)(A) of title 44, United States Code, as*
2 *amended by this Act;*

3 *(2) implementing additional cybersecurity proce-*
4 *dures, which shall include resources for shared serv-*
5 *ices;*

6 *(3) establishing a process for providing the sta-*
7 *tus of each remedial action under section 3554(b)(7)*
8 *of title 44, United States Code, as amended by this*
9 *Act, to the Director and the Cybersecurity and Infra-*
10 *structure Security Agency using automation and ma-*
11 *chine-readable data, as practicable, which shall in-*
12 *clude—*

13 *(A) specific guidance for the use of automa-*
14 *tion and machine-readable data; and*

15 *(B) templates for providing the status of the*
16 *remedial action;*

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

20 *(5) a requirement to coordinate with inspectors*
21 *general of agencies to ensure consistent understanding*
22 *and application of agency policies for the purpose of*
23 *evaluations by inspectors general.*

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

3 (a) *DEFINITIONS.—In this section:*

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

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

12 (b) *GUIDANCE ON NOTIFICATION OF REPORTING ENTI-*
13 *TIES.—Not later than 180 days after the date of enactment*
14 *of this Act, the Director shall issue guidance requiring the*
15 *head of each agency to notify a reporting entity of an inci-*
16 *dent that is likely to substantially affect—*

17 (1) *the confidentiality or integrity of sensitive*
18 *information submitted by the reporting entity to the*
19 *agency pursuant to a statutory or regulatory require-*
20 *ment; or*

21 (2) *the agency information system or systems*
22 *used in the transmission or storage of the sensitive in-*
23 *formation described in paragraph (1).*

1 **TITLE II—IMPROVING FEDERAL**
2 **CYBERSECURITY**

3 **SEC. 201. MOBILE SECURITY STANDARDS.**

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

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

8 (2) *issue guidance to secure mobile devices, in-*
9 *cluding for mobile applications, for every agency.*

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

12 (1) *a requirement, pursuant to section*
13 *3506(b)(4) of title 44, United States Code, for every*
14 *agency to maintain a continuous inventory of*
15 *every—*

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

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

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

24 (c) *INFORMATION SHARING.*—The Director, in coordi-
25 *nation with the Director of the Cybersecurity and Infra-*

1 *structure Security Agency, shall issue guidance to agencies*
2 *for sharing the inventory of the agency required under sub-*
3 *section (b)(1) with the Director of the Cybersecurity and*
4 *Infrastructure Security Agency, using automation and ma-*
5 *chine-readable data to the greatest extent practicable.*

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

12 **SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT**
13 **RESPONSE.**

14 *(a) RECOMMENDATIONS.—Not later than 2 years after*
15 *the date of enactment of this Act, and not less frequently*
16 *than every 2 years thereafter, the Director of the Cybersecu-*
17 *rity and Infrastructure Security Agency, in consultation*
18 *with the Attorney General, shall submit to the Director rec-*
19 *ommendations on requirements for logging events on agency*
20 *systems and retaining other relevant data within the sys-*
21 *tems and networks of an agency.*

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

24 *(1) the types of logs to be maintained;*

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

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

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

7 (5) *requirements to ensure that, upon request, in*
8 *a manner that excludes or otherwise reasonably pro-*
9 *TECTS personally identifiable information, and to the*
10 *extent permitted by applicable law (including privacy*
11 *and statistical laws), 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) *requirements to ensure that, subject to com-*
18 *pliance with statistical laws and other relevant data*
19 *protection requirements, the highest level security op-*
20 *erations center of each agency has visibility into all*
21 *agency logs.*

22 (c) *GUIDANCE.—Not later than 90 days after receiving*
23 *the recommendations submitted under subsection (a), the*
24 *Director, in consultation with the Director of the Cybersecu-*
25 *rity and Infrastructure Security Agency and the Attorney*

1 *General, shall, as determined to be appropriate by the Di-*
2 *rector, update guidance to agencies regarding requirements*
3 *for logging, log retention, log management, sharing of log*
4 *data with other appropriate agencies, or any other logging*
5 *activity determined to be appropriate by the Director.*

6 **SEC. 203. CISA AGENCY ADVISORS.**

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

15 (b) *QUALIFICATIONS.*—Each advisor assigned under
16 *subsection (a) shall have knowledge of—*

17 (1) *cybersecurity threats facing agencies, includ-*
18 *ing any specific threats to the assigned agency;*

19 (2) *performing risk assessments of agency sys-*
20 *tems; and*

21 (3) *other Federal cybersecurity initiatives.*

22 (c) *DUTIES.*—The duties of each advisor assigned
23 *under subsection (a) shall include—*

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

1 (2) *serving as an incident response point of con-*
 2 *tact between the assigned agency and the Cybersecu-*
 3 *rity and Infrastructure Security Agency; and*

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

7 (d) *LIMITATION.—An advisor assigned under sub-*
 8 *section (a) shall not be a contractor.*

9 (e) *MULTIPLE ASSIGNMENTS.—One individual advisor*
 10 *may be assigned to multiple agency Chief Information Offi-*
 11 *cers under subsection (a).*

12 **SEC. 204. FEDERAL PENETRATION TESTING POLICY.**

13 (a) *IN GENERAL.—Subchapter II of chapter 35 of title*
 14 *44, United States Code, is amended by adding at the end*
 15 *the following:*

16 **“§ 3559A. Federal penetration testing**

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

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

21 “(2) *RULES OF ENGAGEMENT.—The term ‘rules*
 22 *of engagement’ means a set of rules established by an*
 23 *agency for the use of penetration testing.*

24 “(b) *GUIDANCE.—*

1 “(1) *IN GENERAL.*—*The Director shall issue*
2 *guidance that—*

3 “(A) *requires agencies to use, when and*
4 *where appropriate, penetration testing on agency*
5 *systems; and*

6 “(B) *requires agencies to develop an agency*
7 *operational plan and rules of engagement that*
8 *meet the requirements under subsection (c).*

9 “(2) *PENETRATION TESTING GUIDANCE.*—*The*
10 *guidance issued under this section shall—*

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

13 “(i) *a shared service of the agency or*
14 *another agency; or*

15 “(ii) *an external entity, such as a ven-*
16 *dor; and*

17 “(B) *require agencies to provide the rules of*
18 *engagement and results of penetration testing to*
19 *the Director and the Director of the Cybersecu-*
20 *rity and Infrastructure Security Agency, without*
21 *regard to the status of the entity that performs*
22 *the penetration testing.*

23 “(c) *AGENCY PLANS AND RULES OF ENGAGEMENT.*—
24 *The agency operational plan and rules of engagement of*
25 *an agency shall—*

- 1 “(1) require the agency to—
- 2 “(A) perform penetration testing on the
- 3 high value assets of the agency; or
- 4 “(B) coordinate with the Director of the Cy-
- 5 bersecurity and Infrastructure Security Agency
- 6 to ensure that penetration testing is being per-
- 7 formed;
- 8 “(2) establish guidelines for avoiding, as a result
- 9 of penetration testing—
- 10 “(A) adverse impacts to the operations of
- 11 the agency;
- 12 “(B) adverse impacts to operational envi-
- 13 ronments and systems of the agency; and
- 14 “(C) inappropriate access to data;
- 15 “(3) require the results of penetration testing to
- 16 include feedback to improve the cybersecurity of the
- 17 agency; and
- 18 “(4) include mechanisms for providing consist-
- 19 ently formatted, and, if applicable, automated and
- 20 machine-readable, data to the Director and the Direc-
- 21 tor of the Cybersecurity and Infrastructure Security
- 22 Agency.
- 23 “(d) RESPONSIBILITIES OF CISA.—The Director of the
- 24 Cybersecurity and Infrastructure Security Agency shall—

1 “(1) *establish a process to assess the performance*
2 *of penetration testing by both Federal and non-Fed-*
3 *eral entities that establishes minimum quality con-*
4 *trols for penetration testing;*

5 “(2) *develop operational guidance for instituting*
6 *penetration testing programs at agencies;*

7 “(3) *develop and maintain a centralized capa-*
8 *bility to offer penetration testing as a service to Fed-*
9 *eral and non-Federal entities; and*

10 “(4) *provide guidance to agencies on the best use*
11 *of penetration testing resources.*

12 “(e) *RESPONSIBILITIES OF OMB.—The Director, in*
13 *coordination with the Director of the Cybersecurity and In-*
14 *frastructure Security Agency, shall—*

15 “(1) *not less frequently than annually, inventory*
16 *all Federal penetration testing assets; and*

17 “(2) *develop and maintain a standardized proc-*
18 *ess for the use of penetration testing.*

19 “(f) *PRIORITIZATION OF PENETRATION TESTING RE-*
20 *SOURCES.—*

21 “(1) *IN GENERAL.—The Director, in coordina-*
22 *tion with the Director of the Cybersecurity and Infra-*
23 *structure Security Agency, shall develop a framework*
24 *for prioritizing Federal penetration testing resources*
25 *among agencies.*

1 “(2) *CONSIDERATIONS.*—*In developing the*
2 *framework under this subsection, the Director shall*
3 *consider—*

4 “(A) *agency system risk assessments per-*
5 *formed under section 3554(a)(1)(A);*

6 “(B) *the Federal risk assessment performed*
7 *under section 3553(i);*

8 “(C) *the analysis of Federal incident data*
9 *performed under section 3597; and*

10 “(D) *any other information determined ap-*
11 *propriate by the Director or the Director of the*
12 *Cybersecurity and Infrastructure Security Agen-*
13 *cy.*

14 “(g) *EXCEPTION FOR NATIONAL SECURITY SYS-*
15 *TEMS.*—*The guidance issued under subsection (b) shall not*
16 *apply to national security systems.*

17 “(h) *DELEGATION OF AUTHORITY FOR CERTAIN SYS-*
18 *TEMS.*—*The authorities of the Director described in sub-*
19 *section (b) shall be delegated—*

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

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

24 “(b) *DEADLINE FOR GUIDANCE.*—*Not later than 180*
25 *days after the date of enactment of this Act, the Director*

1 *shall issue the guidance required under section 3559A(b)*
 2 *of title 44, United States Code, as added by subsection (a).*

3 (c) *CLERICAL AMENDMENT.—The table of sections for*
 4 *chapter 35 of title 44, United States Code, is amended by*
 5 *adding after the item relating to section 3559 the following:*
“3559A. Federal penetration testing.”.

6 (d) *PENETRATION TESTING BY THE SECRETARY OF*
 7 *HOMELAND SECURITY.—Section 3553(b) of title 44, United*
 8 *States Code, as amended by section 101, is further amend-*
 9 *ed—*

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

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

14 (3) *by inserting after paragraph (8) the fol-*
 15 *lowing:*

16 “(9) *performing penetration testing with or*
 17 *without advance notice to, or authorization from,*
 18 *agencies, to identify vulnerabilities within Federal in-*
 19 *formation systems; and”.*

20 **SEC. 205. ONGOING THREAT HUNTING PROGRAM.**

21 (a) *THREAT HUNTING PROGRAM.—*

22 (1) *IN GENERAL.—Not later than 540 days after*
 23 *the date of enactment of this Act, the Director of the*
 24 *Cybersecurity and Infrastructure Security Agency*
 25 *shall establish a program to provide ongoing, hypoth-*

1 *esis-driven threat-hunting services on the network of*
2 *each agency.*

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

10 (A) *determine the method for collecting,*
11 *storing, accessing, and analyzing appropriate*
12 *agency data;*

13 (B) *provide on-premises support to agen-*
14 *cies;*

15 (C) *staff threat hunting services;*

16 (D) *allocate available human and financial*
17 *resources to implement the plan; and*

18 (E) *provide input to the heads of agencies*
19 *on the use of—*

20 (i) *more stringent standards under sec-*
21 *tion 11331(c)(1) of title 40, United States*
22 *Code; and*

23 (ii) *additional cybersecurity procedures*
24 *under section 3554 of title 44, United States*
25 *Code.*

1 **(b) REPORTS.**—*The Director of the Cybersecurity and*
2 *Infrastructure Security Agency shall submit to the appro-*
3 *priate 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 required*
7 *under subsection (a)(2), a report on the plan to pro-*
8 *vide 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 under subsection*
13 *(a)(1), a report providing any updates to the plan de-*
14 *veloped under subsection (a)(2); and*

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

21 **SEC. 206. CODIFYING VULNERABILITY DISCLOSURE PRO-**
22 **GRAMS.**

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

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

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

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

5 “(2) *REPORTER.—The term ‘reporter’ means an*
6 *individual that submits a vulnerability report pursu-*
7 *ant to the vulnerability disclosure process of an agen-*
8 *cy.*

9 “(b) *RESPONSIBILITIES OF OMB.—*

10 “(1) *LIMITATION ON LEGAL ACTION.—The Direc-*
11 *tor, in consultation with the Attorney General, shall*
12 *issue guidance to agencies to not recommend or pur-*
13 *sue legal action against a reporter or an individual*
14 *that conducts a security research activity that the*
15 *head of the agency determines—*

16 “(A) *represents a good faith effort to follow*
17 *the vulnerability disclosure policy of the agency*
18 *developed under subsection (d)(2); and*

19 “(B) *is authorized under the vulnerability*
20 *disclosure policy of the agency developed under*
21 *subsection (d)(2).*

22 “(2) *SHARING INFORMATION WITH CISA.—The*
23 *Director, in coordination with the Director of the Cy-*
24 *bersecurity and Infrastructure Security Agency and*
25 *the National Cyber Director, shall issue guidance to*
26 *agencies on sharing relevant information in a con-*

1 *sistent, automated, and machine readable manner*
2 *with the Cybersecurity and Infrastructure Security*
3 *Agency, including—*

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

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

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

17 *“(ii) about which the head of the agen-*
18 *cy believes the Director of the Cybersecurity*
19 *and Infrastructure Security Agency should*
20 *know; and*

21 *“(C) any other information with respect to*
22 *which the head of the agency determines helpful*
23 *or necessary to involve the Cybersecurity and In-*
24 *frastructure Security Agency.*

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

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

8 “(1) *provide support to agencies with respect to*
9 *the implementation of the requirements of this section;*

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

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

17 “(d) *RESPONSIBILITIES OF AGENCIES.—*

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

22 “(A) *an appropriate security contact; and*

23 “(B) *the component of the agency that is re-*
24 *sponsible for the internet accessible services of-*
25 *fered at the domain.*

1 “(2) *VULNERABILITY DISCLOSURE POLICY.*—*The*
2 *head of each agency shall develop and make publicly*
3 *available a vulnerability disclosure policy for the*
4 *agency, which shall—*

5 “(A) *describe—*

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

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

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

14 “(iv) *the disclosure policy of the agency*
15 *for sensitive information;*

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

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

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

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

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

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

9 “(e) PAPERWORK REDUCTION ACT EXEMPTION.—The
10 requirements of subchapter I (commonly known as the ‘Pa-
11 perwork Reduction Act’) shall not apply to a vulnerability
12 disclosure program established under this section.

13 “(f) CONGRESSIONAL REPORTING.—Not later than 90
14 days after the date of enactment of the Federal Information
15 Security Modernization Act of 2021, and annually there-
16 after for a 3-year period, the Director shall provide to the
17 Committee on Homeland Security and Governmental Af-
18 fairs of the Senate and the Committee on Oversight and
19 Reform of the House of Representatives a briefing on the
20 status of the use of vulnerability disclosure policies under
21 this section at agencies, including, with respect to the guid-
22 ance issued under subsection (b)(3), an identification of the
23 agencies that are compliant and not compliant.

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

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

3 “(h) *DELEGATION OF AUTHORITY FOR CERTAIN SYS-*
 4 *TEMS.—The authorities of the Director and the Director of*
 5 *the Cybersecurity and Infrastructure Security Agency de-*
 6 *scribed in this section shall be delegated—*

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

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

11 “(b) *CLERICAL AMENDMENT.—The table of sections for*
 12 *chapter 35 of title 44, United States Code, is amended by*
 13 *adding after the item relating to section 3559A, as added*
 14 *by section 204, the following:*

“3559B. Federal vulnerability disclosure programs.”.

15 **SEC. 207. IMPLEMENTING PRESUMPTION OF COMPROMISE**
 16 **AND LEAST PRIVILEGE PRINCIPLES.**

17 “(a) *GUIDANCE.—Not later than 1 year after the date*
 18 *of enactment of this Act, the Director shall provide an up-*
 19 *date to the appropriate congressional committees on*
 20 *progress in increasing the internal defenses of agency sys-*
 21 *tems, including—*

22 “(1) *shifting away from “trusted networks” to im-*
 23 *plement security controls based on a presumption of*
 24 *compromise;*

1 (2) *implementing principles of least privilege in*
2 *administering information security programs;*

3 (3) *limiting the ability of entities that cause in-*
4 *cidents to move laterally through or between agency*
5 *systems;*

6 (4) *identifying incidents quickly;*

7 (5) *isolating and removing unauthorized entities*
8 *from agency systems quickly;*

9 (6) *otherwise increasing the resource costs for en-*
10 *tities that cause incidents to be successful; and*

11 (7) *a summary of the agency progress reports re-*
12 *quired under subsection (b).*

13 (b) *AGENCY PROGRESS REPORTS.*—*Not later than 1*
14 *year after the date of enactment of this Act, the head of*
15 *each agency shall submit to the Director a progress report*
16 *on implementing an information security program based*
17 *on the presumption of compromise and least privilege prin-*
18 *ciples, which shall include—*

19 (1) *a description of any steps the agency has*
20 *completed, including progress toward achieving re-*
21 *quirements issued by the Director;*

22 (2) *an identification of activities that have not*
23 *yet been completed and that would have the most im-*
24 *mediate security impact; and*

1 (3) a schedule to implement any planned activi-
2 ties.

3 **SEC. 208. AUTOMATION REPORTS.**

4 (a) *OMB REPORT*.—Not later than 180 days after the
5 date of enactment of this Act, the Director shall submit to
6 the appropriate congressional committees a report on the
7 use of automation under paragraphs (1), (5)(C) and (8)(B)
8 of section 3554(b) of title 44, United States Code.

9 (b) *GAO REPORT*.—Not later than 1 year after the
10 date of enactment of this Act, the Comptroller General of
11 the United States shall perform a study on the use of auto-
12 mation and machine readable data across the Federal Gov-
13 ernment for cybersecurity purposes, including the auto-
14 mated updating of cybersecurity tools, sensors, or processes
15 by agencies.

16 **SEC. 209. EXTENSION OF FEDERAL ACQUISITION SECURITY**
17 **COUNCIL.**

18 Section 1328 of title 41, United States Code, is amend-
19 ed by striking “the date that” and all that follows and in-
20 serting “December 31, 2026.”.

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

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

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

3 (2) *by redesignating subparagraph (B) as sub-*
4 *paragraph (C); and*

5 (3) *by inserting after subparagraph (A) the fol-*
6 *lowing:*

7 *“(B) that shall include a dashboard of open*
8 *information security recommendations identified*
9 *in the independent evaluations required by sec-*
10 *tion 3555(a) of title 44, United States Code;*
11 *and”.*

12 ***TITLE III—RISK-BASED BUDGET***
13 ***MODEL***

14 ***SEC. 301. DEFINITIONS.***

15 *In this title:*

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

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

22 (B) *the Committee on Homeland Security*
23 *and the Committee on Appropriations of the*
24 *House of Representatives.*

1 (2) *COVERED AGENCY.*—The term “covered agen-
2 cy” has the meaning given the term “executive agen-
3 cy” in section 133 of title 41, United States Code.

4 (3) *DIRECTOR.*—The term “Director” means the
5 Director of the Office of Management and Budget.

6 (4) *INFORMATION TECHNOLOGY.*—The term “in-
7 formation technology”—

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

10 (B) includes the hardware and software sys-
11 tems of a Federal agency that monitor and con-
12 trol physical equipment and processes of the Fed-
13 eral agency.

14 (5) *RISK-BASED BUDGET.*—The term “risk-based
15 budget” means a budget—

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

23 (B) that allocates resources based on the
24 risks identified and prioritized under subpara-
25 graph (A).

1 **SEC. 302. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.**

2 (a) *IN GENERAL.*—

3 (1) *MODEL.*—Not later than 1 year after the
4 first publication of the budget submitted by the Presi-
5 dent under section 1105 of title 31, United States
6 Code, following the date of enactment of this Act, the
7 Director, in consultation with the Director of the Cy-
8 bersecurity and Infrastructure Security Agency and
9 the National Cyber Director and in coordination with
10 the Director of the National Institute of Standards
11 and Technology, shall develop a standard model for
12 creating a risk-based budget for cybersecurity spend-
13 ing.

14 (2) *RESPONSIBILITY OF DIRECTOR.*—Section
15 3553(a) of title 44, United States Code, as amended
16 by section 101, is further amended by inserting after
17 paragraph (6) the following:

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

21 (3) *CONTENTS OF MODEL.*—The model required
22 to be developed under paragraph (1) shall—

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

1 (B) consider the impact of agency oper-
2 ations of compromise of systems, including the
3 interconnectivity to other agency systems and the
4 operations of other agencies;

5 (C) indicate where resources should be allo-
6 cated to have the greatest impact on mitigating
7 current and future threats and current and fu-
8 ture cybersecurity capabilities;

9 (D) be used to inform acquisition and
10 sustainment of—

11 (i) information technology and cyberse-
12 curity tools;

13 (ii) information technology and cyber-
14 security architectures;

15 (iii) information technology and cyber-
16 security personnel; and

17 (iv) cybersecurity and information
18 technology concepts of operations; and

19 (E) be used to evaluate and inform Govern-
20 ment-wide cybersecurity programs of the Depart-
21 ment of Homeland Security.

22 (4) *REQUIRED UPDATES.*—Not less frequently
23 than once every 3 years, the Director shall review,
24 and update as necessary, the model required to be de-
25 veloped under this subsection.

1 (5) *PUBLICATION.*—*The Director shall publish*
2 *the model required to be developed under this sub-*
3 *section, and any updates necessary under paragraph*
4 *(4), on the public website of the Office of Management*
5 *and Budget.*

6 (6) *REPORTS.*—*Not later than 1 year after the*
7 *date of enactment of this Act, and annually thereafter*
8 *for each of the 2 following fiscal years or until the*
9 *date on which the model required to be developed*
10 *under this subsection is completed, whichever is soon-*
11 *er, the Director shall submit a report to Congress on*
12 *the development of the model.*

13 (b) *REQUIRED USE OF RISK-BASED BUDGET*
14 *MODEL.*—

15 (1) *IN GENERAL.*—*Not later than 2 years after*
16 *the date on which the model developed under sub-*
17 *section (a) is published, the head of each covered*
18 *agency shall use the model to develop the annual cy-*
19 *bersecurity and information technology budget re-*
20 *quests of the agency.*

21 (2) *AGENCY PERFORMANCE PLANS.*—*Section*
22 *3554(d)(2) of title 44, United States Code, is amended*
23 *by inserting “and the risk-based budget model re-*
24 *quired under section 3553(a)(7)” after “paragraph*
25 *(1)”.*

1 (c) *VERIFICATION.*—

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

4 (A) *in the matter preceding subclause (I),*
5 *by striking “by agency, and by initiative area*
6 *(as determined by the administration)” and in-*
7 *serting “and by agency”;*

8 (B) *in subclause (III), by striking “and” at*
9 *the end; and*

10 (C) *by adding at the end the following:*

11 “(V) *a validation that the budgets*
12 *submitted were developed using a risk-*
13 *based methodology; and*

14 “(VI) *a report on the progress of*
15 *each agency on closing recommenda-*
16 *tions identified under the independent*
17 *evaluation required by section*
18 *3555(a)(1) of title 44.”.*

19 (2) *EFFECTIVE DATE.*—*The amendments made*
20 *by paragraph (1) shall take effect on the date that is*
21 *2 years after the date on which the model developed*
22 *under subsection (a) is published.*

23 (d) *REPORTS.*—

1 (1) *INDEPENDENT EVALUATION.*—Section
2 3555(a)(2) of title 44, United States Code, is amend-
3 ed—

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

6 (B) in subparagraph (C), by striking the
7 period at the end and inserting “; and”; and

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

9 “(D) an assessment of how the agency im-
10 plemented the risk-based budget model required
11 under section 3553(a)(7) and an evaluation of
12 whether the model mitigates agency cyber
13 vulnerabilities.”.

14 (2) *ASSESSMENT.*—Section 3553(c) of title 44,
15 United States Code, as amended by section 101, is
16 further amended by inserting after paragraph (5) the
17 following:

18 “(6) an assessment of—

19 “(A) Federal agency implementation of the
20 model required under subsection (a)(7);

21 “(B) how cyber vulnerabilities of Federal
22 agencies changed from the previous year; and

23 “(C) whether the model mitigates the cyber
24 vulnerabilities of the Federal Government.”.

1 (e) *GAO REPORT.*—Not later than 3 years after the
 2 date on which the first budget of the President is submitted
 3 to Congress containing the validation required under sec-
 4 tion 1105(a)(35)(A)(i)(V) of title 31, United States Code,
 5 as amended by subsection (c), the Comptroller General of
 6 the United States shall submit to the appropriate congres-
 7 sional committees a report that includes—

8 (1) an evaluation of the success of covered agen-
 9 cies in developing risk-based budgets;

10 (2) an evaluation of the success of covered agen-
 11 cies in implementing risk-based budgets;

12 (3) an evaluation of whether the risk-based budg-
 13 ets developed by covered agencies mitigate cyber vul-
 14 nerability, including the extent to which the risk-
 15 based budgets inform Federal Government-wide cyber-
 16 security programs; and

17 (4) any other information relating to risk-based
 18 budgets the Comptroller General determines appro-
 19 priate.

20 **TITLE IV—PILOT PROGRAMS TO**
 21 **ENHANCE FEDERAL CYBERSE-**
 22 **CURITY**

23 **SEC. 401. ACTIVE CYBER DEFENSIVE STUDY.**

24 (a) *DEFINITION.*—In this section, the term “active de-
 25 fense technique”—

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

5 (2) includes a honeypot, deception, or purpose-
6 fully feeding false or misleading data to an adversary
7 when the adversary is on the systems of the entity.

8 (b) *STUDY*.—Not later than 180 days after the date
9 of enactment of this Act, the Director of the Cybersecurity
10 and Infrastructure Security Agency, in coordination with
11 the Director, shall perform a study on the use of active de-
12 fense techniques to enhance the security of agencies, which
13 shall include—

14 (1) a review of legal restrictions on the use of
15 different active cyber defense techniques in Federal
16 environments, in consultation with the Department of
17 Justice;

18 (2) an evaluation of—

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

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

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, concepts*
5 *of operations, and governance plans.*

6 (d) *PILOT PROGRAM.—*

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

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

20 (e) *BRIEFING AND REPORT.—*

21 (1) *BRIEFING.—Not later than 260 days after*
22 *the date of enactment of this Act, the Director of the*
23 *Cybersecurity and Infrastructure Security Agency*
24 *shall provide to the Committee on Homeland Security*
25 *and Governmental Affairs of the Senate and the Com-*

1 *mittee on Homeland Security and the Committee on*
2 *Oversight and Reform of the House of Representatives*
3 *a briefing on the parameters of any 1-year agree-*
4 *ments entered into under subsection (d)(1).*

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

14 (A) *the agreement; and*

15 (B) *any additional agreements entered into*
16 *with agencies under subsection (d).*

Calendar No. 673

117TH CONGRESS
2^D SESSION

S. 2902

[Report No. 117-274]

A BILL

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

DECEMBER 19, 2022

Reported with an amendment