

AMENDMENT NO. _____ Calendar No. _____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

S. 2902

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

Referred to the Committee on _____ and
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended
to be proposed by Mr. PETERS (for himself and Mr.
PORTMAN)

Viz:

1 Strike all after the enacting clause and insert the fol-

2 lowing:

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal Information

5 Security Modernization Act of 2021”.

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

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

Sec. 1. Short title.

Sec. 2. Table of contents.

Sec. 3. Definitions.

TITLE I—UPDATES TO FISMA

Sec. 101. Title 44 amendments.

Sec. 102. Amendments to subtitle III of title 40.

Sec. 103. Actions to enhance Federal incident response.

Sec. 104. Additional guidance to agencies on FISMA updates.

Sec. 105. Agency requirements to notify 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.**—The term “additional cybersecurity procedure” has the meaning given the term in section
 4
 5
 6 3552(b) of title 44, United States Code, as amended
 7 by this Act.

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

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

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

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

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

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

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

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

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

21 (8) THREAT HUNTING.—The term “threat
22 hunting” means proactively and iteratively searching
23 for threats to systems that evade detection by auto-
24 mated threat detection systems.

1 **TITLE I—UPDATES TO FISMA**

2 **SEC. 101. TITLE 44 AMENDMENTS.**

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

5 (1) in section 3504—

6 (A) in subsection (a)(1)(B)—

7 (i) by striking clause (v) and inserting
8 the following:

9 “(v) confidentiality, disclosure, and sharing
10 of information;”;

11 (ii) by redesignating clause (vi) as
12 clause (vii); and

13 (iii) by inserting after clause (v) the
14 following:

15 “(vi) in consultation with the National
16 Cyber Director and the Director of the Cyberse-
17 curity and Infrastructure Security Agency, se-
18 curity of information; and”;

19 (B) in subsection (g), by striking para-
20 graph (1) and inserting the following:

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

23 “(A) develop and oversee the implementa-
24 tion of policies, principles, standards, and

1 guidelines on privacy, confidentiality, disclosure,
2 and sharing of the information; and

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

9 (C) in subsection (h)(1)—

10 (i) in the matter preceding subpara-
11 graph (A)—

12 (I) by inserting “the Director of
13 the Cybersecurity and Infrastructure
14 Security Agency and the National
15 Cyber Director,” before “the Direc-
16 tor”; and

17 (II) by inserting a comma before
18 “and the Administrator”; and

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

22 (2) in section 3505—

23 (A) in paragraph (3) of the first subsection
24 designated as subsection (c)—

25 (i) in subparagraph (B)—

6

1 (I) by inserting “the Director of
2 the Cybersecurity and Infrastructure
3 Security Agency, the National Cyber
4 Director, and” before “the Comp-
5 troller General”; and

6 (II) by striking “and” at the end;

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

10 (iii) by adding at the end the fol-
11 lowing:

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

15 (B) by striking the second subsection des-
16 igned as subsection (c);

17 (3) in section 3506—

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

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

22 (4) in section 3513—

23 (A) by redesignating subsection (c) as sub-
24 section (d); and

1 (B) by inserting after subsection (b) the
2 following:

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

8 (b) SUBCHAPTER II DEFINITIONS.—

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

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

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

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

22 (C) by inserting after paragraph (6), as so
23 redesignated, the following:

24 “(7) The term ‘high value asset’ means infor-
25 mation or an information system that the head of an

1 agency determines so critical to the agency that the
2 loss or corruption of the information or the loss of
3 access to the information system would have a seri-
4 ous impact on the ability of the agency to perform
5 the mission of the agency or conduct business.

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

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

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

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

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

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

24 “(12) The term ‘shared service’ means a cen-
25 tralized business or mission capability that is pro-

1 vided to multiple organizations within an agency or
2 to multiple agencies.”.

3 (2) CONFORMING AMENDMENTS.—

4 (A) HOMELAND SECURITY ACT OF 2002.—

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

9 (B) TITLE 10.—

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

14 (ii) SECTION 2223.—Section
15 2223(c)(3) of title 10, United States Code,
16 is amended by striking “section
17 3552(b)(6)” and inserting “section
18 3552(b)”.

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

23 (iv) SECTION 2339A.—Section
24 2339a(e)(5) of title 10, United States
25 Code, is amended by striking “section

1 3552(b)(6)” and inserting “section
2 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.
6 5527(a)) 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)
11 of the Internet of Things Cybersecurity Im-
12 provement Act of 2020 (15 U.S.C. 278g–3a) is
13 amended by striking “section 3552(b)(6)” and
14 inserting “section 3552(b)”.

15 (E) NATIONAL DEFENSE AUTHORIZATION
16 ACT FOR FISCAL YEAR 2013.—Section
17 933(e)(1)(B) of the National Defense Author-
18 ization Act for Fiscal Year 2013 (10 U.S.C.
19 2224 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
6 3542(b)(2)” and inserting “section
7 3552(b)”;

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

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

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

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

24 (ii) in subsection (f)—

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

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

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

10 (1) in section 3551—

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

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

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

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

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

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

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

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

10 “(10) recognize that—

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

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

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

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

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

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

3 (2) in section 3553—

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 **riety Agency**”.

9 (B) in subsection (a)—

10 (i) in paragraph (1), by inserting “in
11 coordination with the Director of the Cy-
12 bersecurity and Infrastructure Security
13 Agency and the National Cyber Director,”
14 before “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
6 Federal cybersecurity and visibility with respect
7 to the implementation of Federal cybersecurity;
8 and

9 “(B) the use of presumption of com-
10 promise and least privilege principles to improve
11 resiliency and timely response actions to inci-
12 dents on Federal systems.”;

13 (C) in subsection (b)—

14 (i) by striking the subsection heading
15 and inserting “CYBERSECURITY AND IN-
16 FRASTRUCTURE SECURITY AGENCY”;

17 (ii) in the matter preceding paragraph
18 (1), by striking “The Secretary, in con-
19 sultation with the Director” and inserting
20 “‘The Director of the Cybersecurity and In-
21 frastructure Security Agency, in consulta-
22 tion with the Director and the National
23 Cyber Director”;

24 (iii) in paragraph (2)—

1 (I) in subparagraph (A), by in-
2 sserting “and reporting requirements
3 under subchapter IV of this title”
4 after “section 3556”; and

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

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

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

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

23 (D) in subsection (c)—

24 (i) in the matter preceding paragraph
25 (1), by striking “each year” and inserting

1 “each year during which agencies are re-
2 quired to submit reports under section
3 3554(e)”;

4 (ii) by striking paragraph (1);

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

8 (iv) in paragraph (3), as so redesign-
9 nated, by striking “and” at the end;

10 (v) by inserting after paragraph (3),
11 as so redesignated the following:

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

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

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.—On an ongoing
22 and continuous basis, the Director of the Cybersecurity
23 and Infrastructure Security Agency shall perform assess-
24 ments of Federal risk posture using any available informa-
25 tion on the cybersecurity posture of agencies, and brief

1 the Director and National Cyber Director on the findings
2 of those assessments 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 agency compliance with standards
19 issued under section 11331 of title 40;

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

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

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

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

23 (3) in section 3554—

24 (A) in subsection (a)—

25 (i) in paragraph (1)—

1 (I) by redesignating subpara-
2 graphs (A), (B), and (C) as subpara-
3 graphs (B), (C), and (D), respectively;

4 (II) by inserting before subpara-
5 graph (B), as so redesignated, the fol-
6 lowing:

7 “(A) on an ongoing and continuous basis,
8 performing agency system risk assessments
9 that—

10 “(i) identify and document the high
11 value assets of the agency using guidance
12 from the Director;

13 “(ii) evaluate the data assets inven-
14 toried under section 3511 of title 44 for
15 sensitivity to compromises in confiden-
16 tiality, integrity, and availability;

17 “(iii) identify agency systems that
18 have access to or hold the data assets
19 inventoried under section 3511 of title 44;

20 “(iv) evaluate the threats facing agen-
21 cy systems and data, including high value
22 assets, based on Federal and non-Federal
23 cyber threat intelligence products, where
24 available;

1 “(v) evaluate the vulnerability of
2 agency systems and data, including high
3 value assets, including by analyzing—

4 “(I) the results of penetration
5 testing performed by the Department
6 of Homeland Security under section
7 3553(b)(9);

8 “(II) the results of penetration
9 testing performed under section
10 3559A;

11 “(III) information provided to
12 the agency through the vulnerability
13 disclosure program of the agency
14 under section 3559B;

15 “(IV) incidents; and

16 “(V) any other vulnerability in-
17 formation relating to agency systems
18 that is known to the agency;

19 “(vi) assess the impacts of potential
20 agency incidents to agency systems, data,
21 and operations based on the evaluations
22 described in clauses (ii) and (iv) and the
23 agency systems identified under clause
24 (iii); and

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

3 “(E) providing an update on the ongoing
4 and continuous assessment performed under
5 subparagraph (A)—

6 “(i) upon request, to the inspector
7 general of the agency or the Comptroller
8 General of the United States; and

9 “(ii) on a periodic basis, as deter-
10 mined by guidance issued by the Director
11 but not less frequently than annually, to—

12 “(I) the Director;

13 “(II) the Director of the Cyberse-
14 curity and Infrastructure Security
15 Agency; and

16 “(III) the National Cyber Direc-
17 tor;

18 “(F) in consultation with the Director of
19 the Cybersecurity and Infrastructure Security
20 Agency and not less frequently than once every
21 3 years, performing an evaluation of whether
22 additional cybersecurity procedures are appro-
23 priate for securing a system of, or under the
24 supervision of, the agency, which shall—

1 “(i) be completed considering the
2 agency system risk assessment performed
3 under subparagraph (A); and

4 “(ii) include a specific evaluation for
5 high value assets;

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

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

14 “(ii) the Director; and

15 “(iii) the National Cyber Director;

16 and

17 “(H) if the head of the agency determines
18 there is need for additional cybersecurity proce-
19 dures, ensuring that those additional cybersecu-
20 rity procedures are reflected in the budget re-
21 quest of the agency in accordance with the risk-
22 based cyber budget model developed pursuant
23 to section 3553(a)(7);”;

24 (ii) in paragraph (2)—

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

6 (II) in subparagraph (B)—

7 (aa) by striking “in accord-
8 ance with standards” and insert-
9 ing “in accordance with—

10 “(i) standards”; and

11 (bb) by adding at the end
12 the following:

13 “(ii) the evaluation performed under
14 paragraph (1)(F); and

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

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

23 (iii) in paragraph (3)—

24 (I) in subparagraph (A)—

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

3 (bb) in clause (iv), by add-
4 ing “and” at the end; and

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

7 “(v) ensure that—

8 “(I) senior agency information
9 security officers of component agen-
10 cies carry out responsibilities under
11 this subchapter, as directed by the
12 senior agency information security of-
13 ficer of the agency or an equivalent
14 official; and

15 “(II) senior agency information
16 security officers of component agen-
17 cies report to—

18 “(aa) the senior information
19 security officer of the agency or
20 an equivalent official; and

21 “(bb) the Chief Information
22 Officer of the component agency
23 or an equivalent official;”; and

24 (iv) in paragraph (5), by inserting
25 “and the Director of the Cybersecurity and

1 Infrastructure Security Agency” before
2 “on the effectiveness”;

3 (B) in subsection (b)—

4 (i) by striking paragraph (1) and in-
5 serting the following:

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

12 (ii) in paragraph (2)—

13 (I) by striking subparagraph (B)
14 and inserting the following:

15 “(B) comply with the risk-based cyber
16 budget model developed pursuant to section
17 3553(a)(7);” and

18 (II) in subparagraph (D)—

19 (aa) by redesignating
20 clauses (iii) and (iv) as clauses
21 (iv) and (v), respectively;

22 (bb) by inserting after
23 clause (ii) the following:

24 “(iii) binding operational directives
25 and emergency directives promulgated by

1 the Director of the Cybersecurity and In-
2 frastructure Security Agency under section
3 3553;” and

4 (cc) in clause (iv), as so re-
5 designated, by striking “as deter-
6 mined by the agency; and” and
7 inserting “as determined by the
8 agency, considering—

9 “(I) the agency risk assessment
10 performed under subsection (a)(1)(A);
11 and

12 “(II) the determinations of ap-
13 plying more stringent standards and
14 additional cybersecurity procedures
15 pursuant to section 11331(c)(1) of
16 title 40; and”;

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

20 (iv) in paragraph (6), by striking
21 “planning, implementing, evaluating, and
22 documenting” and inserting “planning and
23 implementing and, in consultation with the
24 Director of the Cybersecurity and Infra-

1 structure Security Agency, evaluating and
2 documenting”;

3 (v) by redesignating paragraphs (7)
4 and (8) as paragraphs (8) and (9), respec-
5 tively;

6 (vi) by inserting after paragraph (6)
7 the following:

8 “(7) a process for providing the status of every
9 remedial action and known system vulnerability to
10 the Director and the Director of the Cybersecurity
11 and Infrastructure Security Agency, using automa-
12 tion and machine-readable data to the greatest ex-
13 tent practicable;” and

14 (vii) in paragraph (8)(C), as so redес-
15 igned—

16 (I) by striking clause (ii) and in-
17 serting the following:

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

22 (II) by redesignating clause (iii)
23 as clause (iv);

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

1 “(iii) performing the notifications and
2 other activities required under subchapter
3 IV of this title; and”; and

4 (IV) in clause (iv), as so redesign-
5 nated—

6 (aa) in subclause (I), by
7 striking “and relevant Offices of
8 Inspector General”;

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

11 (cc) by striking subclause
12 (III); and

13 (dd) by redesignating sub-
14 clause (IV) as subclause (III);

15 (C) in subsection (c)—

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

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

20 “(1) BIENNIAL REPORT.—Not later than 2
21 years after the date of enactment of the Federal In-
22 formation Security Modernization Act of 2021 and
23 not less frequently than once every 2 years there-
24 after, using the continuous and ongoing agency sys-
25 tem risk assessment under subsection (a)(1)(A), the

1 head of each agency shall submit to the Director,
2 the Director of the Cybersecurity and Infrastructure
3 Security Agency, the Committee on Homeland Security
4 and Governmental Affairs of the Senate, the
5 Committee on Oversight and Reform of the House
6 of Representatives, the Committee on Homeland Security
7 of the House of Representatives, the appropriate
8 authorization and appropriations committees
9 of Congress, the National Cyber Director, and the
10 Comptroller General of the United States a report
11 that—

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

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

21 “(C) summarizes the evaluation and imple-
22 mentation plans described in subparagraphs (F)
23 and (G) of subsection (a)(1) and whether those
24 evaluation and implementation plans call for
25 the use of additional cybersecurity procedures

1 determined to be appropriate by the agency;
2 and

3 “(D) summarizes the status of remedial
4 actions identified by inspector general of the
5 agency, the Comptroller General of the United
6 States, and any other source determined appro-
7 priate by the head of the agency.

8 “(2) UNCLASSIFIED REPORTS.—Each report
9 submitted under paragraph (1)—

10 “(A) shall be, to the greatest extent prac-
11 ticable, in an unclassified and otherwise uncon-
12 trolled form; and

13 “(B) may include a classified annex.

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

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

1 (iii) in paragraph (5), as so redesignated,
2 nated, by inserting “including the reporting
3 ing procedures established under section
4 11315(d) of title 40 and subsection
5 (a)(3)(A)(v) of this section”; and
6 (D) in subsection (d)—

7 (i) in paragraph (1), in the matter
8 preceding subparagraph (A), by inserting
9 “and the Director of the Cybersecurity and
10 Infrastructure Security Agency” after “the
11 Director”; and

12 (ii) in paragraph (2) by inserting “,
13 including the reporting procedures established
14 under section 11315(d) of title 40
15 and subsection (a)(3)(A)(v) of this section,
16 ” after “practices”;

17 (4) in section 3555—

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

21 (B) in subsection (a)—

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

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

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

8 “(3) An evaluation under this section may include
9 recommendations for improving the cybersecurity posture
10 of the agency.”;

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

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

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

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

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

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

9 “(A) specific information system incidents; or

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

12 (F) in subsection (g)(2)—

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

15 “(A) shall”;

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

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

21 “(B) identify any entity that performs an inde-
22 pendent evaluation under subsection (b).”; and

23 (G) by striking subsection (j) and inserting
24 the following:

25 “(j) GUIDANCE.—

1 “(1) IN GENERAL.—The Director, in consulta-
2 tion with the Director of the Cybersecurity and In-
3 frastructure Security Agency, the Chief Information
4 Officers Council, the Council of the Inspectors Gen-
5 eral on Integrity and Efficiency, and other interested
6 parties as appropriate, shall ensure the development
7 of guidance for evaluating the effectiveness of an in-
8 formation security program and practices

9 “(2) PRIORITIES.—The guidance developed
10 under paragraph (1) shall prioritize the identifica-
11 tion of—

12 “(A) the most common threat patterns ex-
13 perienced by each agency;

14 “(B) the security controls that address the
15 threat patterns described in subparagraph (A);
16 and

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

19 (5) in section 3556(a)—

20 (A) in the matter preceding paragraph (1),
21 by inserting “within the Cybersecurity and In-
22 frastructure Security Agency” after “incident
23 center”; and

24 (B) in paragraph (4), by striking
25 “3554(b)” and inserting “3554(a)(1)(A)”.

1 (d) CONFORMING AMENDMENTS.—

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

5 (A) by striking the item relating to section
6 3553 and inserting the following:

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

7 (B) by striking the item relating to section
8 3555 and inserting the following:

“3555. Independent evaluation.”.

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

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

18 (B) in paragraph (2)(B), in the matter
19 preceding clause (i)—

20 (i) by striking “annually thereafter”
21 and inserting “thereafter during the years
22 during which a report is required to be

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

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

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

10 (e) 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 REPORTING ENTITIES.—The
23 term ‘appropriate reporting entities’ means—

24 “(A) the majority and minority leaders of
25 the Senate;

1 “(B) the Speaker and minority leader of
2 the House of Representatives;

3 “(C) the Committee on Homeland Security
4 and Governmental Affairs of the Senate;

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

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

9 “(F) the appropriate authorization and ap-
10 propriations committees of Congress;

11 “(G) the Director;

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

14 “(I) the National Cyber Director;

15 “(J) the Comptroller General of the United
16 States; and

17 “(K) the inspector general of any impacted
18 agency.

19 “(2) AWARDEE.—The term ‘awardee’—

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

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

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

5 “(A) a compromise of the security, con-
6 fidentiality, or integrity of data in electronic
7 form that results in unauthorized access to, or
8 an acquisition of, personal information; or

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

12 “(4) CONTRACTOR.—The term ‘contractor’
13 means—

14 “(A) a prime contractor of an agency or a
15 subcontractor of a prime contractor of an agen-
16 cy; and

17 “(B) any person or business that collects
18 or maintains information, including personally
19 identifiable information, on behalf of an agency.

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

1 “(6) FEDERAL INFORMATION SYSTEM.—The
2 term ‘Federal information system’ means an infor-
3 mation system used or operated by an agency, a con-
4 tractor, or another organization on behalf of an
5 agency.

6 “(7) INTELLIGENCE COMMUNITY.—The term
7 ‘intelligence community’ has the meaning given the
8 term in section 3 of the National Security Act of
9 1947 (50 U.S.C. 3003).

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

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

18 **“§ 3592. Notification of breach**

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

1 “(1) determine whether notice to any individual
2 potentially affected by the breach is appropriate
3 based on an assessment of the risk of harm to the
4 individual that considers—

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

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

11 “(C) the type of breach; and

12 “(D) any other factors determined by the
13 Director; and

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

17 “(A) to the last known mailing address of
18 the individual; or

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

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

4 “(1) a brief description of the rationale for the
5 determination that notice should be provided under
6 subsection (a);

7 “(2) if possible, a description of the types of
8 personally identifiable information affected by the
9 breach;

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

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

14 “(B) may include a telephone number or a
15 website;

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

18 “(5) any applicable educational materials relat-
19 ing to what individuals can do in response to a
20 breach that potentially affects their personally iden-
21 tifiable information, including relevant information
22 to contact Federal law enforcement agencies and
23 each nationwide consumer reporting agency; and

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

4 “(c) DELAY OF NOTIFICATION.—

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

9 “(A) impede a criminal investigation or a
10 national security activity;

11 “(B) reveal sensitive sources and methods;

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

13 “(D) hamper security remediation actions.

14 “(2) DOCUMENTATION.—

15 “(A) IN GENERAL.—Any delay under para-
16 graph (1) shall be reported in writing to the Di-
17 rector, the Attorney General, the Director of
18 National Intelligence, the Secretary of Home-
19 land Security, the Director of the Cybersecurity
20 and Infrastructure Security Agency, and the
21 head of the agency and the inspector general of
22 the agency that experienced the breach.

23 “(B) CONTENTS.—A report required under
24 subparagraph (A) shall include a written state-

1 ment from the entity that delayed the notifica-
2 tion explaining the need for the delay.

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

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

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

19 “(e) EXEMPTION FROM NOTIFICATION.—

20 “(1) IN GENERAL.—The head of an agency, in
21 consultation with the inspector general of the agen-
22 cy, may request an exemption from the Director
23 from complying with the notification requirements
24 under subsection (a) if the information affected by
25 the breach is determined by an independent evalua-

1 tion to be unreadable, including, as appropriate, in-
2 stances in which the information is—

3 “(A) encrypted; and

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

7 “(2) APPROVAL.—The Director shall determine
8 whether to grant an exemption requested under
9 paragraph (1) in consultation with—

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

12 “(B) the Attorney General.

13 “(3) DOCUMENTATION.—Any exemption grant-
14 ed by the Director under paragraph (1) shall be re-
15 ported in writing to the head of the agency and the
16 inspector general of the agency that experienced the
17 breach and the Director of the Cybersecurity and In-
18 frastructure Security Agency.

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

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

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

6 **“§ 3593. Congressional and Executive Branch reports**

7 “(a) INITIAL REPORT.—

8 “(1) IN GENERAL.—Not later than 72 hours
9 after an agency has a reasonable basis to conclude
10 that a major incident occurred, the head of the
11 agency impacted by the major incident shall submit
12 to the appropriate reporting entities a written report
13 and, to the extent practicable, provide a briefing to
14 the Committee on Homeland Security and Govern-
15 mental Affairs of the Senate, the Committee on
16 Oversight and Reform of the House of Representa-
17 tives, the Committee on Homeland Security of the
18 House of Representatives, and the appropriate au-
19 thorization and appropriations committees of Con-
20 gress, taking into account—

21 “(A) the information known at the time of
22 the report;

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

1 “(C) the classification level of the informa-
2 tion contained in the report.

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

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

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

23 “(C) if applicable, an assessment of the
24 impacts to the agency, the Federal Government,
25 or the security of the United States, based on

1 information available to agency officials on the
2 date on which the agency submits the report.

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

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

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

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

21 “(4) an estimate of the number of individuals
22 potentially affected by the major incident based on
23 information available to agency officials as of the
24 date 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
10 the update; and

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

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

1 includes information relating to the change in under-
2 standing.

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

8 “(e) DELAY AND EXEMPTION REPORT.—

9 “(1) IN GENERAL.—The Director shall submit
10 to the appropriate notification entities an annual re-
11 port on all notification delays and exemptions grant-
12 ed pursuant to subsections (c) and (d) of section
13 3592.

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

18 “(f) REPORT DELIVERY.—Any written report re-
19 quired to be submitted under this section may be sub-
20 mitted in a paper or electronic format.

21 “(g) THREAT BRIEFING.—

22 “(1) IN GENERAL.—Not later than 7 days after
23 the date on which an agency has a reasonable basis
24 to conclude that a major incident occurred, the head
25 of the agency, jointly with the National Cyber Direc-

1 tor and any other Federal entity determined appro-
2 priate by the National Cyber Director, shall provide
3 a briefing to the congressional committees described
4 in subsection (a)(1) on the threat causing the major
5 incident.

6 “(2) COMPONENTS.—The briefing required
7 under paragraph (1)—

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

10 “(B) may include a classified component.

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

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

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

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

20 “(a) IN GENERAL.—

21 “(1) INCIDENT REPORTING.—The head of each
22 agency shall provide any information relating to any
23 incident, whether the information is obtained by the
24 Federal Government directly or indirectly, to the Cy-

1 bersecurity and Infrastructure Security Agency and
2 the Office of Management and Budget.

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

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

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

12 “(C) in order to protect against a similar
13 incident, identify—

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

17 “(ii) additional necessary safeguards;
18 and

19 “(D) include information to aid in incident
20 response, such as—

21 “(i) a description of the affected sys-
22 tems or networks;

23 “(ii) the estimated dates of when the
24 incident occurred; and

1 “(iii) information that could reason-
2 ably help identify the party that conducted
3 the incident.

4 “(3) INFORMATION SHARING.—To the greatest
5 extent practicable, the Director of the Cybersecurity
6 and Infrastructure Security Agency shall share in-
7 formation relating to an incident with any agencies
8 that may be impacted by the incident.

9 “(4) NATIONAL SECURITY SYSTEMS.—Each
10 agency operating or exercising control of a national
11 security system shall share information about inci-
12 dents with the Director of the Cybersecurity and In-
13 frastructure Security Agency to the extent consistent
14 with standards and guidelines for national security
15 systems issued in accordance with law and as di-
16 rected by the President.

17 “(b) COMPLIANCE.—The information provided under
18 subsection (a) shall take into account the level of classi-
19 fication of the information and any information sharing
20 limitations and protections, such as limitations and protec-
21 tions relating to law enforcement, national security, pri-
22 vacy, statistical confidentiality, or other factors deter-
23 mined by the Director

24 “(c) INCIDENT RESPONSE.—Each agency that has a
25 reasonable basis to conclude that a major incident oc-

1 curred involving Federal information in electronic medium
2 or form, as defined by the Director and not involving a
3 national security system, regardless of delays from notifi-
4 cation granted for a major incident, shall coordinate with
5 the Cybersecurity and Infrastructure Security Agency re-
6 garding—

7 “(1) incident response and recovery; and

8 “(2) recommendations for mitigating future in-
9 cidents.

10 **“§ 3595. Responsibilities of contractors and awardees**

11 “(a) NOTIFICATION.—

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

20 “(A) an incident or breach has occurred
21 with respect to Federal information collected,
22 used, or maintained by the contractor or award-
23 ee in connection with the contract, grant, or co-
24 operative agreement of the contractor or award-
25 ee;

1 “(B) an incident or breach has occurred
2 with respect to a Federal information system
3 used or operated by the contractor or awardee
4 in connection with the contract, grant, or coop-
5 erative agreement of the contractor or awardee;
6 or

7 “(C) the contractor or awardee has re-
8 ceived information from the agency that the
9 contractor or awardee is not authorized to re-
10 ceive in connection with the contract, grant, or
11 cooperative agreement of the contractor or
12 awardee.

13 “(2) PROCEDURES.—

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

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

1 quirements under section 3594 with respect to
2 the incident.

3 “(b) EFFECTIVE DATE.—This section shall apply on
4 and after the date that is 1 year after the date of enact-
5 ment of the Federal Information Security Modernization
6 Act of 2021.

7 **“§ 3596. Training**

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

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

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

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

24 “(c) INCLUSION IN ANNUAL TRAINING.—The train-
25 ing developed under subsection (b) may be included as

1 part of an annual privacy or security awareness training
2 of an agency.

3 **“§ 3597. Analysis and report on Federal incidents**

4 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

12 “(A) the causes of incidents, 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 incidents at
19 agencies;

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

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

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

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

8 “(3) 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 and the Na-
12 tional Cyber Director to—

13 “(i) improve the understanding of cy-
14 bersecurity risk of agencies; and

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

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

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

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

1 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—
2 Not later than 2 years after the date of enactment of this
3 section, and not less frequently than annually thereafter,
4 the Director of the Cybersecurity and Infrastructure Secu-
5 rity Agency, in consultation with the Director and other
6 Federal agencies as appropriate, shall submit to the ap-
7 propriate notification entities a report that includes—

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

11 “(2) the quantitative and qualitative analyses of
12 incidents developed under subsection (a)(1), includ-
13 ing specific analysis of breaches, on an agency-by-
14 agency basis and comprehensively across the Federal
15 Government; and

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

17 “(A) a description of each major incident;
18 and

19 “(B) the total number of compromises of
20 the agency.

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

1 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

6 “(2) NONCOMPLIANCE REPORTS.—

7 “(A) IN GENERAL.—Subject to subpara-
8 graph (B), during any year during which the
9 head of an agency does not provide data for an
10 incident to the Cybersecurity and Infrastructure
11 Security Agency in accordance with section
12 3594(a), the head of the agency, in coordina-
13 tion with the Director of the Cybersecurity and
14 Infrastructure Security Agency and the Direc-
15 tor, shall submit to the appropriate reporting
16 entities a report that includes—

17 “(i) data for the incident; and

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

20 “(B) EXCEPTION FOR NATIONAL SECURITY
21 SYSTEMS.—The head of an agency that owns or
22 exercises control of a national security system
23 shall not include data for an incident that oc-
24 curs on a national security system in any report
25 submitted under subparagraph (A).

1 “(3) NATIONAL SECURITY SYSTEM REPORTS.—

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

11 “(i) the the majority and minority
12 leaders of the Senate,

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

15 “(iii) the Committee on Homeland Se-
16 curity and Governmental Affairs of the
17 Senate;

18 “(iv) the Select Committee on Intel-
19 ligence of the Senate;

20 “(v) the Committee on Armed Serv-
21 ices of the Senate;

22 “(vi) the Committee on Oversight and
23 Reform of the House of Representatives;

24 “(vii) the Committee on Homeland
25 Security of the House of Representatives;

1 “(viii) the Permanent Select Com-
2 mittee on Intelligence of the House of Rep-
3 resentatives; and

4 “(ix) the Committee on Armed Serv-
5 ices of the House of Representatives.

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

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

17 “§ 3598. Major incident definition

18 “(a) IN GENERAL.—Not later than 180 days after
19 the date of enactment of the Federal Information Security
20 Modernization Act of 2021, the Director, in coordination
21 with the Director of the Cybersecurity and Infrastructure
22 Security Agency and the National Cyber Director, shall
23 develop and promulgate guidance on the definition of the
24 term ‘major incident’ for the purposes of subchapter II
25 and this subchapter.

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

4 “(1) include, with respect to any information
5 collected or maintained by or on behalf of an agency
6 or an information system used or operated by an
7 agency or by a contractor of an agency or another
8 organization on behalf of an agency—

9 “(A) any incident the head of the agency
10 determines is likely to have an impact on—

11 “(i) the national security, homeland
12 security, or economic security of the
13 United States; or

14 “(ii) the civil liberties or public health
15 and safety of the people of the United
16 States;

17 “(B) any incident the head of the agency
18 determines likely to result in an inability for the
19 agency, a component of the agency, or the Fed-
20 eral Government, to provide 1 or more critical
21 services;

22 “(C) any incident that the head of an
23 agency, in consultation with a senior privacy of-
24 ficer of the agency, determines is likely to have

1 a significant privacy impact on 1 or more indi-
2 vidual;

3 “(D) any incident that the head of the
4 agency, in consultation with a senior privacy of-
5 ficial of the agency, determines is likely to have
6 a substantial privacy impact on a significant
7 number of individuals;

8 “(E) any incident the head of the agency
9 determines impacts the operations of a high
10 value asset owned or operated by the agency;

11 “(F) any incident involving the exposure of
12 sensitive agency information to a foreign entity,
13 such as the communications of the head of the
14 agency, the head of a component of the agency,
15 or the direct reports of the head of the agency
16 or the head of a component of the agency; and

17 “(G) any other type of incident determined
18 appropriate by the Director;

19 “(2) stipulate that the National Cyber Director
20 shall declare a major incident at each agency im-
21 pacted by an incident if the Director of the Cyberse-
22 curity and Infrastructure Security Agency deter-
23 mines that an incident—

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

25 and

1 “(B)(i) is enabled by a common technical
2 root cause, such as a supply chain compromise,
3 a common software or hardware vulnerability;
4 or

5 “(ii) is enabled by the related activities of
6 a common threat actor; and

7 “(3) stipulate that, in determining whether an
8 incident constitutes a major incident because that
9 incident—

10 “(A) is any incident described in para-
11 graph (1), the head of an agency shall consult
12 with the Director of the Cybersecurity and In-
13 frastructure Security Agency;

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

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

20 “(i) the Privacy and Civil Liberties
21 Oversight Board; and

22 “(ii) the Executive Director of the
23 Federal Trade Commission.

1 “(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In de-
2 termining what constitutes a significant number of indi-
3 viduals under subsection (b)(1)(D), the Director—

4 “(1) may determine a threshold for a minimum
5 number of individuals that constitutes a significant
6 amount; and

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

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

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

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

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

1 (2) CLERICAL AMENDMENT.—The table of sec-
 2 tions for chapter 35 of title 44, United States Code,
 3 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.”.

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

5 (a) INFORMATION TECHNOLOGY MODERNIZATION
 6 CENTERS OF EXCELLENCE PROGRAM ACT.—Section
 7 2(c)(4)(A)(ii) of the Information Technology Moderniza-
 8 tion Centers of Excellence Program Act (40 U.S.C. 11301
 9 note) is amended by striking the period at the end and
 10 inserting “, which shall be provided in coordination with
 11 the Director of the Cybersecurity and Infrastructure Secu-
 12 rity Agency.”.

13 (b) MODERNIZING GOVERNMENT TECHNOLOGY.—
 14 Subtitle G of title X of Division A of the National Defense
 15 Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301
 16 note) is amended—

17 (1) in section 1077(b)—

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

21 (B) in paragraph (7)—

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

3 (ii) by striking “In evaluating
4 projects” and inserting the following:

5 “(A) CONSIDERATION OF GUIDANCE.—In
6 evaluating projects”;

7 (iii) in subparagraph (A), as so des-
8 ignated, by striking “under section
9 1094(b)(1)” and inserting “by the Direc-
10 tor”; and

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

13 “(B) CONSULTATION.—In using funds
14 under paragraph (3)(A), the Chief Information
15 Officer of the covered agency shall consult with
16 the necessary stakeholders to ensure the project
17 appropriately addresses cybersecurity risks, in-
18 cluding the Director of the Cybersecurity and
19 Infrastructure Security Agency, as appro-
20 priate.”; and

21 (2) in section 1078—

22 (A) by striking subsection (a) and insert-
23 ing the following:

24 “(a) DEFINITIONS.—In this section:

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

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

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

9 “(8) PROPOSAL EVALUATION.—The Director
10 shall—

11 “(A) give consideration for the use of
12 amounts in the Fund to improve the security of
13 high value assets; and

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

20 (C) in subsection (c)—

21 (i) in paragraph (2)(A)(i), by insert-
22 ing “, including a consideration of the im-
23 pact on high value assets” after “oper-
24 ational risks”;

25 (ii) in paragraph (5)—

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

3 (II) in subparagraph (B), by
4 striking the period at the end and in-
5 serting “and”; and

6 (III) by adding at the end the
7 following:

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

12 (iii) in paragraph (6)(A), by striking
13 “shall be—” and all that follows through
14 “4 employees” and inserting “shall be 4
15 employees”.

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

18 (1) in section 11302—

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

25 (B) in subsection (c)—

1 (i) in paragraph (3)—
2 (I) in subparagraph (A)—
3 (aa) by striking “including
4 data” and inserting “which
5 shall—
6 “(i) include data”;
7 (bb) in clause (i), as so des-
8 ignated, by striking “, and per-
9 formance” and inserting “secu-
10 rity, and performance; and”; and
11 (cc) by adding at the end
12 the following:
13 “(ii) specifically denote cybersecurity
14 funding under the risk-based cyber budget
15 model developed pursuant to section
16 3553(a)(7) of title 44.”; and
17 (II) in subparagraph (B), adding
18 at the end the following:
19 “(iii) The Director shall provide to the
20 National Cyber Director any cybersecurity
21 funding information described in subpara-
22 graph (A)(ii) that is provided to the Direc-
23 tor under clause (ii) of this subpara-
24 graph.”; and

1 (ii) in paragraph (4)(B), in the matter
2 preceding clause (i), by inserting “not later
3 than 30 days after the date on which the
4 review under subparagraph (A) is com-
5 pleted,” before “the Administrator”;

6 (C) in subsection (f)—

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

10 “(1) develop”;

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

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

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

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

23 (2) in section 11303(b)—

24 (A) in paragraph (2)(B)—

1 (i) in clause (i), by striking “or” at
2 the end;

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

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

7 “(iii) whether the function should be
8 performed by a shared service offered by
9 another executive agency;”; and

10 (B) in paragraph (5)(B)(i), by inserting “,
11 while taking into account the risk-based cyber
12 budget model developed pursuant to section
13 3553(a)(7) of title 44” after “title 31”.

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

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

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

21 (3) in section 11315, by adding at the end the
22 following:

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

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

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

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

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

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

13 (1) in subsection (a), by striking “section
14 3532(b)(1)” and inserting “section 3552(b)”;

15 (2) in subsection (b)(1)(A)—

16 (A) by striking “in consultation” and in-
17 serting “in coordination”; and

18 (B) by striking “the Secretary of Home-
19 land Security” and inserting “the Director of
20 the Cybersecurity and Infrastructure Security
21 Agency”;

22 (3) by striking subsection (c) and inserting the
23 following:

24 “(c) APPLICATION OF MORE STRINGENT STAND-
25 ARDS.—

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

3 “(A) evaluate, in consultation with the sen-
4 ior agency information security officers, the
5 need to employ standards for cost-effective,
6 risk-based information security for all systems,
7 operations, and assets within or under the su-
8 pervision of the agency that are more stringent
9 than the standards promulgated by the Director
10 under this section, if such standards contain, at
11 a minimum, the provisions of those applicable
12 standards made compulsory and binding by the
13 Director; and

14 “(B) to the greatest extent practicable and
15 if the head of the agency determines that the
16 standards described in subparagraph (A) are
17 necessary, employ those standards.

18 “(2) EVALUATION OF MORE STRINGENT STAND-
19 ARDS.—In evaluating the need to employ more strin-
20 gent standards under paragraph (1), the head of an
21 agency shall consider available risk information,
22 such as—

23 “(A) the status of cybersecurity remedial
24 actions of the agency;

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

3 “(C) incident information of the agency;

4 “(D) information from—

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

7 “(ii) information from the vulner-
8 ability disclosure program established
9 under section 3559B of title 44;

10 “(E) agency threat hunting results under
11 section 207 of the Federal Information Security
12 Modernization Act of 2021;

13 “(F) Federal and non-Federal threat intel-
14 ligence;

15 “(G) data on compliance with standards
16 issued under this section;

17 “(H) agency system risk assessments per-
18 formed under section 3554(a)(1)(A) of title 44;
19 and

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

22 (4) in subsection (d)(2)—

23 (A) in the paragraph heading, by striking
24 “NOTICE AND COMMENT” and inserting “CON-
25 SULTATION, NOTICE, AND COMMENT”;

1 (B) by inserting “promulgate,” before
2 “significantly modify”; and

3 (C) by striking “shall be made after the
4 public is given an opportunity to comment on
5 the Director’s proposed decision.” and inserting
6 “shall be made—

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

11 “(B) in consultation with the Chief Infor-
12 mation Officers Council, the Director of the Cy-
13 bersecurity and Infrastructure Security Agency,
14 the National Cyber Director, the Comptroller
15 General of the United States, and the Council
16 of the Inspectors General on Integrity and Effi-
17 ciency;

18 “(C) considering the Federal risk assess-
19 ments performed under section 3553(i) of title
20 44; and

21 “(D) considering the extent to which the
22 proposed standard reduces risk relative to the
23 cost of implementation of the standard.”; and
24 (5) by adding at the end the following:

1 “(e) REVIEW OF OFFICE OF MANAGEMENT AND
2 BUDGET GUIDANCE AND POLICY.—

3 “(1) CONDUCT OF REVIEW.—

4 “(A) IN GENERAL.—Not less frequently
5 than once every 3 years, the Director of the Of-
6 fice of Management and Budget, in consultation
7 with the Chief Information Officers Council, the
8 Director of the Cybersecurity and Infrastruc-
9 ture Security Agency, the National Cyber Di-
10 rector, the Comptroller General of the United
11 States, and the Council of the Inspectors Gen-
12 eral on Integrity and Efficiency shall review the
13 efficacy of the guidance and policy promulgated
14 by the Director in reducing cybersecurity risks,
15 including an assessment of the requirements for
16 agencies to report information to the Director,
17 and determine whether any changes to that
18 guidance or policy is appropriate.

19 “(B) FEDERAL RISK ASSESSMENTS.—In
20 conducting the review described in subpara-
21 graph (A), the Director shall consider the Fed-
22 eral risk assessments performed under section
23 3553(i) of title 44.

24 “(2) UPDATED GUIDANCE.—Not later than 90
25 days after the date on which a review is completed

1 under paragraph (1), the Director of the Office of
2 Management and Budget shall issue updated guid-
3 ance or policy to agencies determined appropriate by
4 the Director, based on the results of the review.

5 “(3) PUBLIC REPORT.—Not later than 30 days
6 after the date on which a review is completed under
7 paragraph (1), the Director of the Office of Manage-
8 ment and Budget shall make publicly available a re-
9 port that includes—

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

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

17 “(C) a summary of the guidance or policy
18 to which changes were determined appropriate
19 during the review and what the changes are an-
20 ticipated to include.

21 “(4) CONGRESSIONAL BRIEFING.—Not later
22 than 30 days after the date on which a review is
23 completed under paragraph (1), the Director shall
24 provide to the Committee on Homeland Security and
25 Governmental Affairs of the Senate and the Com-

1 mittee on Oversight and Reform of the House of
2 Representatives a briefing on the review.

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

15 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**
16 **SPONSE.**

17 (a) **RESPONSIBILITIES OF THE CYBERSECURITY AND**
18 **INFRASTRUCTURE SECURITY AGENCY.**—

19 (1) **IN GENERAL.**—Not later than 180 days
20 after the date of enactment of this Act, the Director
21 of the Cybersecurity and Infrastructure Security
22 Agency shall—

23 (A) develop a plan for the development of
24 the analysis required under section 3597(a) of
25 title 44, United States Code, as added by this

1 Act, and the report required under subsection
2 (c) of that section that includes—

3 (i) a description of any challenges the
4 Director anticipates encountering; and

5 (ii) the use of automation and ma-
6 chine-readable formats for collecting, com-
7 piling, monitoring, and analyzing data; and

8 (B) provide to the appropriate congres-
9 sional committees a briefing on the plan devel-
10 oped under subparagraph (A).

11 (2) BRIEFING.—Not later than 1 year after the
12 date of enactment of this Act, the Director of the
13 Cybersecurity and Infrastructure Security Agency
14 shall provide to the appropriate congressional com-
15 mittees a briefing on—

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

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

21 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
22 OFFICE OF MANAGEMENT AND BUDGET.—

23 (1) FISMA.—Section 2 of the Federal Informa-
24 tion Security Modernization Act of 2014 (44 U.S.C.
25 3554 note) is amended—

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

2 (B) by redesignating subsections (c)
3 through (f) as subsections (b) through (e), re-
4 spectively.

5 (2) INCIDENT DATA SHARING.—

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

12 (B) REQUIREMENTS.—The guidance devel-
13 oped under subparagraph (A) shall—

14 (i) prioritize the availability of data
15 necessary to understand and analyze—

16 (I) the causes of incidents;

17 (II) the scope and scale of inci-
18 dents within the environments and
19 systems of an agency;

20 (III) a root cause analysis of in-
21 cidents that—

22 (aa) are common across the
23 Federal Government; or

24 (bb) have a Government-
25 wide impact;

1 (IV) agency response, recovery,
2 and remediation actions and the effec-
3 tiveness of those actions; and

4 (V) the impact of incidents;

5 (ii) enable the efficient development
6 of—

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

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

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

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

20 (3) GUIDANCE ON RESPONDING TO INFORMA-
21 TION REQUESTS.—Not later than 1 year after the
22 date of enactment of this Act, the Director shall de-
23 velop guidance for agencies to implement the re-
24 quirement under section 3594(c) of title 44, United

1 States Code, as added by this Act, to provide infor-
2 mation to other agencies experiencing incidents.

3 (4) STANDARD GUIDANCE AND TEMPLATES.—

4 Not later than 1 year after the date of enactment
5 of this Act, the Director, in consultation with the
6 Director of the Cybersecurity and Infrastructure Se-
7 curity Agency, shall develop guidance and templates,
8 to be reviewed and, if necessary, updated not less
9 frequently than once every 2 years, for use by Fed-
10 eral agencies in the activities required under sections
11 3592, 3593, and 3596 of title 44, United States
12 Code, as added by this Act.

13 (5) CONTRACTOR AND GRANTEE GUIDANCE.—

14 (A) IN GENERAL.—Not later than 1 year
15 after the date of enactment of this Act, the Di-
16 rector, in coordination with the Secretary of
17 Homeland Security, the Secretary of Defense,
18 the Administrator of General Services, and the
19 heads of other agencies determined appropriate
20 by the Director, shall issue guidance to Federal
21 agencies on how to deconflict, to the greatest
22 extent practicable, existing regulations, policies,
23 and procedures relating to the responsibilities of
24 contractors and awardees established under sec-

1 tion 3595 of title 44, United States Code, as
2 added by this Act.

3 (B) EXISTING PROCESSES.—To the great-
4 est extent practicable, the guidance issued
5 under subparagraph (A) shall allow contractors
6 and awardees to use existing processes for noti-
7 fying Federal agencies of incidents involving in-
8 formation of the Federal Government.

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

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

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

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

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

22 “(13) to another agency in furtherance of a re-
23 sponse to an incident (as defined in section 3552 of
24 title 44) and pursuant to the information sharing re-
25 quirements in section 3594 of title 44 if the head of

1 the requesting agency has made a written request to
2 the agency that maintains the record specifying the
3 particular portion desired and the activity for which
4 the record is sought.”.

5 **SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**
6 **UPDATES.**

7 Not later than 1 year after the date of enactment
8 of this Act, the Director, in coordination with the Director
9 of the Cybersecurity and Infrastructure Security Agency,
10 shall issue guidance for agencies on—

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

15 (2) implementing additional cybersecurity pro-
16 cedures, which shall include resources for shared
17 services;

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

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

3 (B) templates for providing the status of
4 the remedial action;

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

8 (5) a requirement to coordinate with inspectors
9 general of agencies to ensure consistent under-
10 standing and application of agency policies for the
11 purpose of evaluations by inspectors general.

12 **SEC. 105. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**
13 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

14 (a) DEFINITIONS.—In this section:

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

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

22 (b).

23 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-
24 TITIES.—Not later than 180 days after the date of enact-
25 ment of this Act, the Director shall issue guidance requir-

1 ing the head of each agency to notify a reporting entity
2 of an incident that is likely to substantially affect—

3 (1) the confidentiality or integrity of sensitive
4 information submitted by the reporting entity to the
5 agency pursuant to a statutory or regulatory re-
6 quirement; or

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

10 **TITLE II—IMPROVING FEDERAL** 11 **CYBERSECURITY**

12 **SEC. 201. MOBILE SECURITY STANDARDS.**

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

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

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

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

21 (1) a requirement, pursuant to section
22 3506(b)(4) of title 44, United States Code, for every
23 agency to maintain a continuous inventory of
24 every—

1 (A) mobile device operated by or on behalf
2 of the agency; and

3 (B) vulnerability identified by the agency
4 associated with a mobile device; and

5 (2) a requirement for every agency to perform
6 continuous evaluation of the vulnerabilities described
7 in paragraph (1)(B) and other risks associated with
8 the use of applications on mobile devices.

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

17 (d) BRIEFING.—Not later than 60 days after the date
18 on which the Director issues guidance under subsection
19 (a)(2), the Director, in coordination with the Director of
20 the Cybersecurity and Infrastructure Security Agency,
21 shall provide to the appropriate congressional committees
22 a briefing on the guidance.

1 **SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT**
2 **RESPONSE.**

3 (a) RECOMMENDATIONS.—Not later than 2 years
4 after the date of enactment of this Act, and not less fre-
5 quently than every 2 years thereafter, the Director of the
6 Cybersecurity and Infrastructure Security Agency, in con-
7 sultation with the Attorney General, shall submit to the
8 Director recommendations on requirements for logging
9 events on agency systems and retaining other relevant
10 data within the systems and networks of an agency.

11 (b) CONTENTS.—The recommendations provided
12 under subsection (a) shall include—

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

14 (2) the time periods to retain the logs and other
15 relevant data;

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

18 (4) how to ensure the confidentiality, integrity,
19 and availability of logs;

20 (5) requirements to ensure that, upon request,
21 in a manner that excludes or otherwise reasonably
22 protects personally identifiable information, and to
23 the extent permitted by applicable law (including
24 privacy and statistical laws), agencies provide logs
25 to—

1 (A) the Director of the Cybersecurity and
2 Infrastructure Security Agency for a cybersecu-
3 rity purpose; and

4 (B) the Federal Bureau of Investigation to
5 investigate potential criminal activity; and

6 (6) requirements to ensure that, subject to com-
7 pliance with statistical laws and other relevant data
8 protection requirements, the highest level security
9 operations center of each agency has visibility into
10 all agency logs.

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

21 **SEC. 203. CISA AGENCY ADVISORS.**

22 (a) IN GENERAL.—Not later than 120 days after the
23 date of enactment of this Act, the Director of the Cyberse-
24 curity and Infrastructure Security Agency shall assign not
25 less than 1 cybersecurity professional employed by the Cy-

1 bersecurity and Infrastructure Security Agency to be the
2 Cybersecurity and Infrastructure Security Agency advisor
3 to the senior agency information security officer of each
4 agency.

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

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

9 (2) performing risk assessments of agency sys-
10 tems; and

11 (3) other Federal cybersecurity initiatives.

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

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

16 (2) serving as an incident response point of
17 contact between the assigned agency and the Cyber-
18 security and Infrastructure Security Agency; and

19 (3) familiarizing themselves with agency sys-
20 tems, processes, and procedures to better facilitate
21 support to the agency in responding to incidents.

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

1 (e) MULTIPLE ASSIGNMENTS.—One individual advi-
2 sor may be assigned to multiple agency Chief Information
3 Officers under subsection (a).

4 **SEC. 204. FEDERAL PENETRATION TESTING POLICY.**

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

8 **“§ 3559A. Federal penetration testing**

9 “(a) DEFINITIONS.—In this section:

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

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

17 “(b) GUIDANCE.—

18 “(1) IN GENERAL.—The Director shall issue
19 guidance that—

20 “(A) requires agencies to use, when and
21 where appropriate, penetration testing on agen-
22 cy systems; and

23 “(B) requires agencies to develop an agen-
24 cy operational plan and rules of engagement

1 that meet the requirements under subsection
2 (c).

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

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

7 “(i) a shared service of the agency or
8 another agency; or

9 “(ii) an external entity, such as a ven-
10 dor; and

11 “(B) require agencies to provide the rules
12 of engagement and results of penetration test-
13 ing to the Director and the Director of the Cy-
14 bersecurity and Infrastructure Security Agency,
15 without regard to the status of the entity that
16 performs the penetration testing.

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

20 “(1) require the agency to—

21 “(A) perform penetration testing on the
22 high value assets of the agency; or

23 “(B) coordinate with the Director of the
24 Cybersecurity and Infrastructure Security

1 Agency to ensure that penetration testing is
2 being performed;

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

5 “(A) adverse impacts to the operations of
6 the agency;

7 “(B) adverse impacts to operational envi-
8 ronments and systems of the agency; and

9 “(C) inappropriate access to data;

10 “(3) require the results of penetration testing
11 to include feedback to improve the cybersecurity of
12 the agency; and

13 “(4) include mechanisms for providing consist-
14 ently formatted, and, if applicable, automated and
15 machine-readable, data to the Director and the Di-
16 rector of the Cybersecurity and Infrastructure Secu-
17 rity Agency.

18 “(d) RESPONSIBILITIES OF CISA.—The Director of
19 the Cybersecurity and Infrastructure Security Agency
20 shall—

21 “(1) establish a process to assess the perform-
22 ance of penetration testing by both Federal and non-
23 Federal entities that establishes minimum quality
24 controls for penetration testing;

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

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

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

8 “(e) RESPONSIBILITIES OF OMB.—The Director, in
9 coordination with the Director of the Cybersecurity and
10 Infrastructure Security Agency, shall—

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

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

15 “(f) PRIORITIZATION OF PENETRATION TESTING RE-
16 SOURCES.—

17 “(1) IN GENERAL.—The Director, in coordina-
18 tion with the Director of the Cybersecurity and In-
19 frastructure Security Agency, shall develop a frame-
20 work for prioritizing Federal penetration testing re-
21 sources among agencies.

22 “(2) CONSIDERATIONS.—In developing the
23 framework under this subsection, the Director shall
24 consider—

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

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

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

7 “(D) any other information determined ap-
8 propriate by the Director or the Director of the
9 Cybersecurity and Infrastructure Security
10 Agency.

11 “(g) EXCEPTION FOR NATIONAL SECURITY SYS-
12 TEMS.—The guidance issued under subsection (b) shall
13 not apply to national security systems.

14 “(h) DELEGATION OF AUTHORITY FOR CERTAIN
15 SYSTEMS.—The authorities of the Director described in
16 subsection (b) shall be delegated—

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

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

21 (b) DEADLINE FOR GUIDANCE.—Not later than 180
22 days after the date of enactment of this Act, the Director
23 shall issue the guidance required under section 3559A(b)
24 of title 44, United States Code, as added by subsection
25 (a).

1 (c) CLERICAL AMENDMENT.—The table of sections
2 for chapter 35 of title 44, United States Code, is amended
3 by adding after the item relating to section 3559 the fol-
4 lowing:

“3559A. Federal penetration testing.”.

5 (d) PENETRATION TESTING BY THE SECRETARY OF
6 HOMELAND SECURITY.—Section 3553(b) of title 44,
7 United States Code, as amended by section 101, is further
8 amended—

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

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

13 (3) by inserting after paragraph (8) the fol-
14 lowing:

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

19 **SEC. 205. ONGOING THREAT HUNTING PROGRAM.**

20 (a) THREAT HUNTING PROGRAM.—

21 (1) IN GENERAL.—Not later than 540 days
22 after the date of enactment of this Act, the Director
23 of the Cybersecurity and Infrastructure Security
24 Agency shall establish a program to provide ongoing,

1 hypothesis-driven threat-hunting services on the net-
2 work of each agency.

3 (2) PLAN.—Not later than 180 days after the
4 date of enactment of this Act, the Director of the
5 Cybersecurity and Infrastructure Security Agency
6 shall develop a plan to establish the program re-
7 quired under paragraph (1) that describes how the
8 Director of the Cybersecurity and Infrastructure Se-
9 curity 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
21 section 11331(c)(1) of title 40, United
22 States Code; and

23 (ii) additional cybersecurity proce-
24 dures under section 3554 of title 44,
25 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 under sub-
13 section (a)(1), a report providing any updates to the
14 plan developed under subsection (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. 206. CODIFYING VULNERABILITY DISCLOSURE PRO-**
2 **GRAMS.**

3 (a) IN GENERAL.—Chapter 35 of title 44, United
4 States Code, is amended by inserting after section 3559A,
5 as added by section 204 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 of the
24 agency developed under subsection (d)(2); and

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

4 “(2) SHARING INFORMATION WITH CISA.—The
5 Director, in coordination with the Director of the
6 Cybersecurity and Infrastructure Security Agency
7 and the National Cyber Director, shall issue guid-
8 ance to agencies on sharing relevant information in
9 a consistent, automated, and machine readable man-
10 ner with the Cybersecurity and Infrastructure Secu-
11 rity Agency, including—

12 “(A) any valid or credible reports of newly
13 discovered or not publicly known vulnerabilities
14 (including misconfigurations) on Federal infor-
15 mation systems that use commercial software or
16 services;

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

21 “(i) with which the head of the agency
22 believes the Director of the Cybersecurity
23 and Infrastructure Security Agency can as-
24 sist; or

1 “(ii) about which the head of the
2 agency believes the Director of the Cyber-
3 security and Infrastructure Security Agen-
4 cy should know; and

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

9 “(3) AGENCY VULNERABILITY DISCLOSURE
10 POLICIES.—The Director shall issue guidance to
11 agencies on the required minimum scope of agency
12 systems covered by the vulnerability disclosure policy
13 of an agency required under subsection (d)(2).

14 “(c) RESPONSIBILITIES OF CISA.—The Director of
15 the Cybersecurity and Infrastructure Security Agency
16 shall—

17 “(1) provide support to agencies with respect to
18 the implementation of the requirements of this sec-
19 tion;

20 “(2) develop tools, processes, and other mecha-
21 nisms determined appropriate to offer agencies capa-
22 bilities to implement the requirements of this sec-
23 tion; and

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

4 “(d) RESPONSIBILITIES OF AGENCIES.—

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

9 “(A) an appropriate security contact; and

10 “(B) the component of the agency that is
11 responsible for the internet accessible services
12 offered at the domain.

13 “(2) VULNERABILITY DISCLOSURE POLICY.—
14 The head of each agency shall develop and make
15 publicly available a vulnerability disclosure policy for
16 the agency, which shall—

17 “(A) describe—

18 “(i) the scope of the systems of the
19 agency included in the vulnerability disclo-
20 sure policy;

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

23 “(iii) the type of information system
24 testing that is not authorized by the agen-
25 cy; and

1 “(iv) the disclosure policy of the agen-
2 cy for sensitive information;

3 “(B) with respect to a report to an agency,
4 describe—

5 “(i) how the reporter should submit
6 the report; and

7 “(ii) if the report is not anonymous,
8 when the reporter should anticipate an ac-
9 knowledgment of receipt of the report by
10 the agency;

11 “(C) include any other relevant informa-
12 tion; and

13 “(D) be mature in scope, to cover all Fed-
14 eral information systems used or operated by
15 that agency or on behalf of that agency.

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

21 “(e) PAPERWORK REDUCTION ACT EXEMPTION.—
22 The requirements of subchapter I (commonly known as
23 the ‘Paperwork Reduction Act’) shall not apply to a vul-
24 nerability disclosure program established under this sec-
25 tion.

1 “(f) CONGRESSIONAL REPORTING.—Not later than
2 90 days after the date of enactment of the Federal Infor-
3 mation Security Modernization Act of 2021, and annually
4 thereafter for a 3-year period, the Director shall provide
5 to the Committee on Homeland Security and Govern-
6 mental Affairs of the Senate and the Committee on Over-
7 sight and Reform of the House of Representatives a brief-
8 ing on the status of the use of vulnerability disclosure poli-
9 cies under this section at agencies, including, with respect
10 to the guidance issued under subsection (b)(3), an identi-
11 fication of the agencies that are compliant and not compli-
12 ant.

13 “(g) EXEMPTIONS.—The authorities and functions of
14 the Director and Director of the Cybersecurity and Infra-
15 structure Security Agency under this section shall not
16 apply to national security systems.

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

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

23 “(2) to the Director of National Intelligence in
24 the case of systems described in section
25 3553(e)(3).”.

1 (b) CLERICAL AMENDMENT.—The table of sections
2 for chapter 35 of title 44, United States Code, is amended
3 by adding after the item relating to section 3559A, as
4 added by section 204, the following:

“3559B. Federal vulnerability disclosure programs.”.

5 **SEC. 207. IMPLEMENTING PRESUMPTION OF COMPROMISE**
6 **AND LEAST PRIVILEGE PRINCIPLES.**

7 (a) GUIDANCE.—Not later than 1 year after the date
8 of enactment of this Act, the Director shall provide an
9 update to the appropriate congressional committees on
10 progress in increasing the internal defenses of agency sys-
11 tems, including—

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

15 (2) implementing principles of least privilege in
16 administering information security programs;

17 (3) limiting the ability of entities that cause in-
18 cidents to move laterally through or between agency
19 systems;

20 (4) identifying incidents quickly;

21 (5) isolating and removing unauthorized entities
22 from agency systems quickly;

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

1 (7) a summary of the agency progress reports
2 required under subsection (b).

3 (b) **AGENCY PROGRESS REPORTS.**—Not later than 1
4 year after the date of enactment of this Act, the head of
5 each agency shall submit to the Director a progress report
6 on implementing an information security program based
7 on the presumption of compromise and least privilege
8 principles, which shall include—

9 (1) a description of any steps the agency has
10 completed, including progress toward achieving re-
11 quirements issued by the Director;

12 (2) an identification of activities that have not
13 yet been completed, which would have the most im-
14 mediate security impact; and

15 (3) a schedule to implement any planned activi-
16 ties.

17 **SEC. 208. 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 (8)(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. 209. EXTENSION OF FEDERAL ACQUISITION SECURITY**
7 **COUNCIL.**

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

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

13 (a) DASHBOARD REQUIRED.—Section 11(e)(2) of the
14 Inspector General Act of 1978 (5 U.S.C. App.) is amend-
15 ed—

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

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

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

22 “(B) that shall include a dashboard of
23 open information security recommendations
24 identified in the independent evaluations re-

1 quired by section 3555(a) of title 44, United
2 States Code; and”.

3 **TITLE III—RISK-BASED BUDGET**
4 **MODEL**

5 **SEC. 301. DEFINITIONS.**

6 In this title:

7 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**
8 **TEES.**—The term “appropriate congressional com-
9 mittees” means—

10 (A) the Committee on Homeland Security
11 and Governmental Affairs and the Committee
12 on Appropriations of the Senate; and

13 (B) the Committee on Homeland Security
14 and the Committee on Appropriations of the
15 House of Representatives.

16 (2) **COVERED AGENCY.**—The term “covered
17 agency” has the meaning given the term “executive
18 agency” in section 133 of title 41, United States
19 Code.

20 (3) **DIRECTOR.**—The term “Director” means
21 the Director of the Office of Management and Budg-
22 et.

23 (4) **INFORMATION TECHNOLOGY.**—The term
24 “information technology”—

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

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

7 (5) RISK-BASED BUDGET.—The term “risk-
8 based budget” means a budget—

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

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

19 **SEC. 302. ESTABLISHMENT OF RISK-BASED BUDGET**
20 **MODEL.**

21 (a) IN GENERAL.—

22 (1) MODEL.—Not later than 1 year after the
23 first publication of the budget submitted by the
24 President under section 1105 of title 31, United
25 States Code, following the date of enactment of this

1 Act, the Director, in consultation with the Director
2 of the Cybersecurity and Infrastructure Security
3 Agency and the National Cyber Director and in co-
4 ordination with the Director of the National Insti-
5 tute of Standards and Technology, shall develop a
6 standard model for creating a risk-based budget for
7 cybersecurity spending.

8 (2) RESPONSIBILITY OF DIRECTOR.—Section
9 3553(a) of title 44, United States Code, as amended
10 by section 101, is further amended by inserting after
11 paragraph (6) the following:

12 “(7) developing a standard risk-based budget
13 model to inform Federal agency cybersecurity budget
14 development; and”.

15 (3) CONTENTS OF MODEL.—The model re-
16 quired to be developed under paragraph (1) shall—

17 (A) consider Federal and non-Federal
18 cyber threat intelligence products, where avail-
19 able, to identify threats, vulnerabilities, and
20 risks;

21 (B) consider the impact of agency oper-
22 ations of compromise of systems, including the
23 interconnectivity to other agency systems and
24 the operations of other agencies;

1 (C) indicate where resources should be al-
2 located to have the greatest impact on miti-
3 gating current and future threats and current
4 and future cybersecurity capabilities;

5 (D) be used to inform acquisition and
6 sustainment of—

7 (i) information technology and cyber-
8 security tools;

9 (ii) information technology and cyber-
10 security architectures;

11 (iii) information technology and cyber-
12 security personnel; and

13 (iv) cybersecurity and information
14 technology concepts of operations; and

15 (E) be used to evaluate and inform govern-
16 ment-wide cybersecurity programs of the De-
17 partment of Homeland Security.

18 (4) REQUIRED UPDATES.—Not less frequently
19 than once every 3 years, the Director shall review,
20 and update as necessary, the model required to be
21 developed under this subsection.

22 (5) PUBLICATION.—The Director shall publish
23 the model required to be developed under this sub-
24 section, and any updates necessary under paragraph

1 (4), on the public website of the Office of Manage-
2 ment and Budget.

3 (6) REPORTS.—Not later than 1 year after the
4 date of enactment of this Act, and annually there-
5 after for each of the 2 following fiscal years or until
6 the date on which the model required to be devel-
7 oped under this subsection is completed, whichever is
8 sooner, the Director shall submit a report to Con-
9 gress on the development of the model.

10 (b) REQUIRED USE OF RISK-BASED BUDGET
11 MODEL.—

12 (1) IN GENERAL.—Not later than 2 years after
13 the date on which the model developed under sub-
14 section (a) is published, the head of each covered
15 agency shall use the model to develop the annual cy-
16 bersecurity and information technology budget re-
17 quests of the agency.

18 (2) AGENCY PERFORMANCE PLANS.—Section
19 3554(d)(2) of title 44, United States Code, is
20 amended by inserting “and the risk-based budget
21 model required under section 3553(a)(7)” after
22 “paragraph (1)”.

23 (c) VERIFICATION.—

24 (1) IN GENERAL.—Section 1105(a)(35)(A)(i) of
25 title 31, United States Code, is amended—

1 (A) in the matter preceding subclause (I),
2 by striking “by agency, and by initiative area
3 (as determined by the administration)” and in-
4 serting “and by agency”;

5 (B) in subclause (III), by striking “and”
6 at the end; and

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

8 “(V) a validation that the budg-
9 ets submitted were developed using a
10 risk-based methodology; and

11 “(VI) a report on the progress of
12 each agency on closing recommenda-
13 tions identified under the independent
14 evaluation required by section
15 3555(a)(1) of title 44.”.

16 (2) EFFECTIVE DATE.—The amendments made
17 by paragraph (1) shall take effect on the date that
18 is 2 years after the date on which the model devel-
19 oped under subsection (a) is published.

20 (d) REPORTS.—

21 (1) INDEPENDENT EVALUATION.—Section
22 3555(a)(2) of title 44, United States Code, is
23 amended—

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

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

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

4 “(D) an assessment of how the agency im-
5 plemented the risk-based budget model required
6 under section 3553(a)(7) and an evaluation of
7 whether the model mitigates agency cyber
8 vulnerabilities.”.

9 (2) ASSESSMENT.—Section 3553(c) of title 44,
10 United States Code, as amended by section 101, is
11 further amended by inserting after paragraph (5)
12 the following:

13 “(6) an assessment of—

14 “(A) Federal agency implementation of the
15 model required under subsection (a)(7);

16 “(B) how cyber vulnerabilities of Federal
17 agencies changed from the previous year; and

18 “(C) whether the model mitigates the
19 cyber vulnerabilities of the Federal Government;
20 and”.

21 (e) GAO REPORT.—Not later than 3 years after the
22 date on which the first budget of the President is sub-
23 mitted to Congress containing the validation required
24 under section 1105(a)(35)(A)(i)(V) of title 31, United
25 States Code, as amended by subsection (c), the Comp-

1 troller General of the United States shall submit to the
2 appropriate congressional committees a report that in-
3 cludes—

4 (1) an evaluation of the success of covered
5 agencies in developing risk-based budgets;

6 (2) an evaluation of the success of covered
7 agencies in implementing risk-based budgets;

8 (3) an evaluation of whether the risk-based
9 budgets developed by covered agencies mitigate
10 cyber vulnerability, including the extent to which the
11 risk-based budgets inform Federal Government-wide
12 cybersecurity programs; and

13 (4) any other information relating to risk-based
14 budgets the Comptroller General determines appro-
15 priate.

16 **TITLE IV—PILOT PROGRAMS TO**
17 **ENHANCE FEDERAL CYBER-**
18 **SECURITY**

19 **SEC. 401. ACTIVE CYBER DEFENSIVE STUDY.**

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

22 (1) means an action taken on the systems of an
23 entity to increase the security of information on the
24 network of an agency by misleading an adversary;
25 and

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

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

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

15 (2) an evaluation of—

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

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

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

1 sure that active defense techniques do not impede
2 threat response efforts, criminal investigations, and
3 national security activities, including intelligence col-
4 lection; and

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

7 **SEC. 402. SECURITY OPERATIONS CENTER AS A SERVICE**
8 **PILOT.**

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

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

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

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

25 (2) staffing and resources; and

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

3 (d) PILOT PROGRAM.—

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

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

18 (e) BRIEFING AND REPORT.—

19 (1) BRIEFING.—Not later than 260 days after
20 the date of enactment of this Act, the Director of
21 the Cybersecurity and Infrastructure Security Agen-
22 cy shall provide to the Committee on Homeland Se-
23 curity and Governmental Affairs of the Senate and
24 the Committee on Homeland Security and the Com-
25 mittee on Oversight and Reform of the House of

1 Representatives a briefing on the parameters of any
2 1-year agreements entered into under subsection
3 (d)(1).

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

13 (A) the agreement; and

14 (B) any additional agreements entered into
15 with agencies under subsection (d).