

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

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 entities impacted by incidents.

TITLE II—IMPROVING FEDERAL CYBERSECURITY

- Sec. 201. Evaluation of effectiveness of implementing standards.
- Sec. 202. Mobile security standards.
- Sec. 203. Quantitative cybersecurity metrics.
- Sec. 204. Data and logging retention for incident response.
- Sec. 205. CISA agency advisors.
- Sec. 206. Federal penetration testing policy.
- Sec. 207. Ongoing threat hunting program.
- Sec. 208. Codifying vulnerability disclosure programs.
- Sec. 209. Implementing presumption of compromise and zero trust architectures.
- Sec. 210. Automation reports.
- Sec. 211. Extension of Federal acquisition security council.
- Sec. 212. Council of the Inspectors General on Integrity and Efficiency dashboard.
- Sec. 213. National security and Department of Defense systems.

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. Continuous independent evaluation pilot.
- Sec. 402. Active cyber defensive study.
- Sec. 403. 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.

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

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

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

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

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

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

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

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

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

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

3 **TITLE I—UPDATES TO FISMA**

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

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

7 (1) in section 3504—

8 (A) in subsection (a)(1)(B)—

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

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

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

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

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

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

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

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

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

11 (C) in subsection (h)(1)—

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

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

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

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

24 (2) in section 3505—

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

3 (i) in subparagraph (B)—

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

9 (II) by striking “and” at the end;

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

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

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

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

20 (3) in section 3506—

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

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

25 (4) in section 3513—

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

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

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

10 (b) SUBCHAPTER II DEFINITIONS.—

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

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

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

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

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

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

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

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

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

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

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

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

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

5 (2) CONFORMING AMENDMENTS.—

6 (A) HOMELAND SECURITY ACT OF 2002.—

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

11 (B) TITLE 10.—

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

16 (ii) SECTION 2223.—Section
17 2223(c)(3) of title 10, United States Code,
18 is amended by striking “section
19 3552(b)(6)” and inserting “section
20 3552(b)”.

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

1 (iv) SECTION 2339A.—Section
2 2339a(e)(5) of title 10, United States
3 Code, is amended by striking “section
4 3552(b)(6)” and inserting “section
5 3552(b)”.

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

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

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

24 (F) IKE SKELTON NATIONAL DEFENSE AU-
25 THORIZATION ACT FOR FISCAL YEAR 2011.—The

1 Ike Skelton National Defense Authorization Act
2 for Fiscal Year 2011 (Public Law 111–383) is
3 amended—

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

7 (ii) in section 931(b)(3) (10 U.S.C.
8 2223 note), by striking “section
9 3542(b)(2)” and inserting “section
10 3552(b)”;

11 (iii) in section 932(b)(2) (10 U.S.C.
12 2224 note), by striking “section
13 3542(b)(2)” and inserting “section
14 3552(b)”.

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

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

12

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

4 (ii) in subsection (f)—

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

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

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

14 (1) in section 3551—

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

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

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

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

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

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

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

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

16 “(10) recognize that—

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

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

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

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

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

9 (2) in section 3553—

10 (A) in subsection (a)—

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

16 (ii) in paragraph (5)—

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

22 (II) by striking “and” at the end;

23 and

24 (iii) by adding at the end the fol-
25 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 against
12 incidents on Federal systems.”;

13 (B) 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 (C) in subsection (c)—

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

1 (ii) by redesignating paragraph (5) as
2 paragraph (7); and

3 (iii) by inserting after paragraph (4)
4 the following:

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

7 (D) by redesignating subsections (i), (j),
8 (k), and (l) as subsections (j), (k), (l), and (m)
9 respectively;

10 (E) by inserting after subsection (h) the
11 following:

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

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

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

24 “(3) analysis of incident information under sec-
25 tion 3597;

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

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

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

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

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

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

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

15 (F) in subsection (j), as so redesignated—

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

19 “(1) the specific”;

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

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

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

3 (3) in section 3554—

4 (A) in subsection (a)—

5 (i) in paragraph (1)—

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

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

12 “(A) on an ongoing and continuous basis,
13 performing agency system risk assessments
14 that—

15 “(i) identify and documents the high
16 value assets of the agency using guidance
17 from the Director;

18 “(ii) evaluate the data assets inven-
19 toried under section 3511 of title 44 for
20 sensitivity to compromises in confiden-
21 tiality, integrity, and availability;

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

1 “(iv) evaluate the threats facing agen-
2 cy systems and data, including high value
3 assets, based on Federal and non-Federal
4 cyber threat intelligence products, where
5 available;

6 “(v) evaluate the vulnerability of
7 agency systems and data, including high
8 value assets, including by analyzing—

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

13 “(II) the results of penetration
14 testing performed under section
15 3559A;

16 “(III) information provided to
17 the agency through the vulnerability
18 disclosure program of the agency
19 under section 3559B;

20 “(IV) incidents; and

21 “(V) any other vulnerability in-
22 formation relating to agency systems
23 that is known to the agency;

24 “(vi) assess the impacts of potential
25 agency incidents to agency systems, data,

1 and operations based on the evaluations
2 described in clauses (ii) and (iv) and the
3 agency systems identified under clause
4 (iii); and

5 “(vii) assess the consequences of po-
6 tential incidents occurring on agency sys-
7 tems that would impact systems at other
8 agencies, including due to interconnectivity
9 between different agency systems or oper-
10 ational reliance on the operations of the
11 system or data in the system;”;

12 (III) in subparagraph (B), as so
13 redesignated, in the matter preceding
14 clause (i), by striking “providing in-
15 formation” and inserting “using infor-
16 mation from the assessment con-
17 ducted under subparagraph (A), pro-
18 viding, in coordination with the Direc-
19 tor of the Cybersecurity and Infra-
20 structure Security Agency, informa-
21 tion”;

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

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

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

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

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

11 “(i) upon request, to the inspector
12 general of the agency; and

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

17 “(I) the Director;

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

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

23 “(F) in consultation with the Director of
24 the Cybersecurity and Infrastructure Security
25 Agency and not less frequently than annually,

1 performing an evaluation of whether additional
2 cybersecurity procedures are appropriate for se-
3 curing a system of, or under the supervision of,
4 the agency, which shall—

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

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

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

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

18 “(ii) the Director; and

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

21 “(H) if the head of the agency determines
22 there is need for additional cybersecurity proce-
23 dures, ensuring that those additional cybersecu-
24 rity procedures are reflected in the budget re-
25 quest of the agency in accordance with the risk-

1 based cyber budget model developed pursuant
2 to section 3553(a)(7);”;

3 (ii) in paragraph (2)—

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

9 (II) in subparagraph (B)—

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

13 “(i) standards”; and

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

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

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

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

1 (iii) in paragraph (3)—

2 (I) in subparagraph (A)—

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

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

7 (cc) by adding at the end
8 the following:

9 “(v) ensure that—

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

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

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

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

1 (iv) in paragraph (5), by inserting
2 “and the Director of the Cybersecurity and
3 Infrastructure Security Agency” before
4 “on the effectiveness”;
5 (B) in subsection (b)—

6 (i) by striking paragraph (1) and in-
7 serting the following:

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

14 (ii) in paragraph (2)—

15 (I) by striking subparagraph (B)
16 and inserting the following:

17 “(B) comply with the risk-based cyber
18 budget model developed pursuant to section
19 3553(a)(7);”;

20 (II) in subparagraph (D)—

21 (aa) by redesignating
22 clauses (iii) and (iv) as clauses
23 (iv) and (v), respectively;

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

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

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

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

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

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

22 (iv) in paragraph (6), by striking
23 “planning, implementing, evaluating, and
24 documenting” and inserting “planning and
25 implementing and, in consultation with the

1 Director of the Cybersecurity and Infra-
2 structure Security Agency, evaluating and
3 documenting”;

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

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

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

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

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

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

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

1 (III) by inserting after clause (ii)
2 the following:

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

6 (IV) in clause (iv), as so redesign-
7 nated—

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

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

13 (cc) by striking subclause
14 (III); and

15 (dd) by redesignating sub-
16 clause (IV) as subclause (III);

17 (C) in subsection (c)—

18 (i) by redesignating paragraph (2) as
19 paragraph (4); and

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

22 “(1) BIENNIAL REPORT.—Not later than 2
23 years after the date of enactment of the Federal In-
24 formation Security Modernization Act of 2021 and
25 not less frequently than once every 2 years there-

1 after, using the continuous and ongoing agency sys-
2 tem risk assessment under subsection (a)(1)(A), the
3 head of each agency shall submit to the Director,
4 the Secretary, the Committee on Homeland Security
5 and Governmental Affairs of the Senate, the Com-
6 mittee on Oversight and Reform of the House of
7 Representatives, the Committee on Homeland Secu-
8 rity of the House of Representatives, the appropriate
9 authorization and appropriations committees of Con-
10 gress, the National Cyber Director, and the Comp-
11 troller General of the United States a report that—

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

15 “(B) evaluates the adequacy and effective-
16 ness of information security policies, proce-
17 dures, and practices of the agency to address
18 the risks identified in the 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).”; and

19 (D) in subsection (d)—

20 (i) in paragraph (1), in the matter
21 preceding subparagraph (A), by inserting
22 “and the Director of the Cybersecurity and
23 Infrastructure Security Agency” after “the
24 Director”; and

1 (ii) in paragraph (2) by inserting “,
2 including the reporting procedures estab-
3 lished under section 11315(d) of title 40
4 and subsection (a)(3)(A)(v) of this sec-
5 tion,” after “practices”;

6 (4) in section 3555—

7 (A) in the section heading, by striking
8 “**ANNUAL INDEPENDENT**” and inserting
9 “**INDEPENDENT**”;

10 (B) in subsection (a)—

11 (i) in paragraph (1), by inserting
12 “during which a report is required to be
13 submitted under section 3553(c),” after
14 “Each year”;

15 (ii) in paragraph (2)(A), by inserting
16 “, including by penetration testing and
17 analyzing the vulnerability disclosure pro-
18 gram of the agency” after “information
19 systems”; and

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

22 “(3) An evaluation under this section may include
23 recommendations for improving the cybersecurity posture
24 of the agency.”;

25 (C) in subsection (b)—

1 (i) in the subsection heading, by strik-
2 ing “AUDITOR” and inserting “EVAL-
3 UATOR”;

4 (ii) in paragraph (1)—

5 (I) by striking “annual.”; and

6 (II) by striking “auditor” and in-
7 serting “evaluator”; and

8 (iii) in paragraph (2), by striking
9 “independent external auditor” and insert-
10 ing “independent external evaluator”;

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

14 (E) by striking subsection (f) and inserting
15 the following:

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

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

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

6 “(A) specific information system incidents; or

7 “(B) specific information system
8 vulnerabilities.”;

9 (F) in subsection (g)(2)—

10 (i) by striking “this subsection shall”

11 and inserting “this subsection—

12 “(A) shall”;

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

14 ignated, by striking the period at the end

15 and inserting “; and”; and

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

17 lowing:

18 “(B) identify any entity that performs an inde-

19 pendent evaluation under subsection (b).”; and

20 (G) by striking subsection (j) and inserting

21 the following:

22 “(j) GUIDANCE.—

23 “(1) IN GENERAL.—The Director, in consulta-

24 tion with the Director of the Cyber Security and In-

25 frastructure Security Agency, the Chief Information

1 Officers Council, the Council of the Inspectors Gen-
2 eral on Integrity and Efficiency, and other interested
3 parties as appropriate, shall ensure the development
4 of guidance for evaluating the effectiveness of an in-
5 formation security program and practices

6 “(2) PRIORITIES.—The guidance developed
7 under paragraph (1) shall prioritize the identifica-
8 tion of—

9 “(A) the most common threat patterns ex-
10 perience by each agency;

11 “(B) the security controls that address the
12 threat patterns described in subparagraph (A);
13 and

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

16 (5) in section 3556(a)—

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

21 (B) in paragraph (4), by striking
22 “3554(b)” and inserting “3554(a)(1)(A)”.

23 (d) CONFORMING AMENDMENTS.—

24 (1) TABLE OF SECTIONS.—The table of sections
25 for chapter 35 of title 44, United States Code, is

1 amended by striking the item relating to section
2 3555 and inserting the following:

“3555. Independent evaluation.”.

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

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

12 (B) in paragraph (2)(B), in the matter
13 preceding clause (i)—

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

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

22 (3) NIST RESPONSIBILITIES.—Section
23 20(d)(3)(B) of the National Institute of Standards
24 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is
25 amended by striking “annual”.

1 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

5 “SUBCHAPTER IV—FEDERAL SYSTEM
6 INCIDENT RESPONSE

7 **“SEC. 3591. DEFINITIONS.**

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

11 “(b) ADDITIONAL DEFINITIONS.—As used in this
12 subchapter:

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

15 “(A) the majority and minority leaders of
16 the Senate;

17 “(B) the Speaker and minority leader of
18 the House of Representatives;

19 “(C) the Committee on Homeland Security
20 and Governmental Affairs of the Senate;

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

23 “(E) the Committee on Homeland Security
24 of the House of Representatives;

1 “(F) the appropriate authorization and ap-
2 propriations committees of Congress;

3 “(G) the Director;

4 “(H) the Director of the Cybersecurity and
5 Infrastructure Security Agency;

6 “(I) the National Cyber Director;

7 “(J) the Comptroller General of the United
8 States; and

9 “(K) the inspector general of any impacted
10 agency.

11 “(2) AWARDEE.—The term ‘awardee’—

12 “(A) means a person, business, or other
13 entity that receives a grant from, or is a party
14 to a cooperative agreement with, an agency;
15 and

16 “(B) includes any subgrantee of a person,
17 business, or other entity described in subpara-
18 graph (A).

19 “(3) BREACH.—The term ‘breach’ means an in-
20 cident that causes a high risk to an individual, as
21 determined by the head of an agency in coordination
22 with the Director, due to an exposure of information
23 relating to the individual.

24 “(4) CONTRACTOR.—The term ‘contractor’
25 means—

1 “(A) a prime contractor of an agency or a
2 subcontractor of a prime contractor of an agen-
3 cy; and

4 “(B) any person or business that collects
5 or maintains information, including personally
6 identifiable information, on behalf of an agency.

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

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

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

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

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

4 **“SEC. 3592. NOTIFICATION OF BREACH.**

5 “(a) NOTIFICATION.—As expeditiously as practicable
6 and without unreasonable delay, and in any case not later
7 than 30 days after an agency has a reasonable basis to
8 conclude that a breach has occurred, the head of the agen-
9 cy, in consultation with the senior privacy officer of the
10 agency, shall—

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

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

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

21 “(C) the type of breach; and

22 “(D) any other factors determined by the
23 Director; and

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

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

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

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

14 “(1) a brief description of the rationale for the
15 determination that notice should be provided under
16 subsection (a);

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

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

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

24 “(B) may include a telephone number or a
25 website;

1 “(4) information on any remedy being offered
2 by the agency;

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

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

12 “(c) DELAY OF NOTIFICATION.—

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

17 “(A) impede a criminal investigation or a
18 national security activity;

19 “(B) reveal sensitive sources and methods;

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

21 “(D) hamper security remediation actions.

22 “(2) DOCUMENTATION.—

23 “(A) IN GENERAL.—Any delay under para-
24 graph (1) shall be reported in writing to the Di-
25 rector, the Attorney General, the Director of

1 National Intelligence, the Secretary of Home-
2 land Security, the Director of the Cybersecurity
3 and Infrastructure Security Agency, and the
4 head of the agency and the inspector general of
5 the agency that experienced the breach.

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

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

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

15 “(d) UPDATE NOTIFICATION.—If an agency deter-
16 mines there is a significant change in the reasonable basis
17 to conclude that a breach occurred or that it is necessary
18 to update the details of the information provided to im-
19 pacted individuals as described in subsection (b), the agen-
20 cy shall as expeditiously as practicable and without unrea-
21 sonable delay, and in any case not later than 30 days after
22 such a determination, notify each individual who received
23 a notification pursuant to subsection (a) of those changes.

24 “(e) EXEMPTION FROM NOTIFICATION.—

1 “(1) IN GENERAL.—The head of an agency, in
2 consultation with the inspector general of the agen-
3 cy, may request an exemption from the Director
4 from complying with the notification requirements
5 under subsection (a) if the information affected by
6 the breach is determined by an independent evalua-
7 tion to be unreadable, including, as appropriate, in-
8 stances in which the information is—

9 “(A) encrypted; and

10 “(B) determined by the Director of the Cy-
11 bersecurity and Infrastructure Security Agency
12 to be of sufficiently low risk of exposure.

13 “(2) APPROVAL.—The Director shall determine
14 whether to grant an exemption requested under
15 paragraph (1) in consultation with—

16 “(A) the Director of the Cybersecurity and
17 Infrastructure Security Agency; and

18 “(B) the Attorney General.

19 “(3) DOCUMENTATION.—Any exemption grant-
20 ed by the Director under paragraph (1) shall be re-
21 ported in writing to the head of the agency and the
22 inspector general of the agency that experienced the
23 breach and the Director of the Cybersecurity and In-
24 frastructure Security Agency.

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

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

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

12 **“SEC. 3593. CONGRESSIONAL AND EXECUTIVE BRANCH RE-**
13 **PORTS.**

14 “(a) INITIAL REPORT.—

15 “(1) IN GENERAL.—Not later than 5 days after
16 the date on which an agency has a reasonable basis
17 to conclude that a major incident occurred, the head
18 of the agency impacted by the major incident shall
19 submit to the appropriate reporting entities a writ-
20 ten report and, to the extent practicable, provide a
21 briefing to the Committee on Homeland Security
22 and Governmental Affairs of the Senate, the Com-
23 mittee on Oversight and Reform of the House of
24 Representatives, the Committee on Homeland Secu-
25 rity of the House of Representatives, and the appro-

1 piate authorization and appropriations committees
2 of Congress, taking into account—

3 “(A) the information known at the time of
4 the report;

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

7 “(C) the classification level of the informa-
8 tion contained in the report.

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

15 “(A) a summary of the information avail-
16 able about the major incident, including how
17 the major incident occurred and information re-
18 lating to the major incident as a breach, based
19 on information available to agency officials as
20 of the date on which the agency submits the re-
21 port;

22 “(B) if applicable, a description and any
23 associated documentation of any circumstances
24 necessitating a delay in or exemption to notifi-
25 cation to individuals potentially affected by the

1 major incident under subsection (c) or (e) of
2 section 3592; and

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

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

16 “(1) vulnerabilities, means by which the major
17 incident occurred, and impacts to the agency relat-
18 ing to the major incident;

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

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

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

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

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

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

23 “(c) UPDATE REPORT.—If the agency determines
24 that there is any significant change in the understanding
25 of the agency of the scope, scale, or consequence of a

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

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

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

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

19 “(g) THREAT BRIEFING.—

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

1 a briefing to the congressional committees described
2 in subsection (a)(1) on the threat causing the major
3 incident.

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

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

8 “(B) may include a classified component.

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

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

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

16 “(i) BINDING OPERATIONAL DIRECTIVE.—If the Di-
17 rector of the Cybersecurity and Infrastructure Security
18 Agency issues a binding operational directive or an emer-
19 gency directive under section 3553, not later than 2 days
20 after the date on which the binding operational directive
21 requires an agency to take an action, the Director of the
22 Cybersecurity and Infrastructure Security Agency shall
23 provide to the appropriate reporting entities the status of
24 the implementation of the binding operational directive at
25 the agency.

1 **“SEC. 3594. GOVERNMENT INFORMATION SHARING AND IN-**
2 **CIDENT RESPONSE.**

3 “(a) IN GENERAL.—

4 “(1) INCIDENT REPORTING.—The head of each
5 agency shall provide any information relating to any
6 incident, whether the information is obtained by the
7 Federal Government directly or indirectly, to the Cy-
8 bersecurity and Infrastructure Security Agency and
9 the Office of Management and Budget.

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

13 “(A) include detailed information about
14 the safeguards that were in place when the inci-
15 dent occurred;

16 “(B) whether the agency implemented the
17 safeguards described in subparagraph (A) cor-
18 rectly; and

19 “(C) in order to protect against a similar
20 incident, identify—

21 “(i) how the safeguards described in
22 subparagraph (A) should be implemented
23 differently; and

24 “(ii) additional necessary safeguards.

25 “(3) INFORMATION-SHARING.—To the greatest
26 extent practicable, the Director of the Cybersecurity

1 and Infrastructure Security Agency shall share in-
2 formation relating to an incident with any agencies
3 that may be impacted by the incident.

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

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

19 “(c) INCIDENT RESPONSE.—Each agency that has a
20 reasonable basis to conclude that a major incident oc-
21 curred involving Federal information in electronic medium
22 or form, as defined by the Director and not involving a
23 national security system, regardless of delays from notifi-
24 cation granted for a major incident, shall coordinate with

1 the Cybersecurity and Infrastructure Security Agency re-
2 garding—

3 “(1) incident response and recovery; and

4 “(2) recommendations for mitigating future in-
5 cidents.

6 **“SEC. 3595. RESPONSIBILITIES OF CONTRACTORS AND**
7 **AWARDEES.**

8 “(a) NOTIFICATION.—

9 “(1) IN GENERAL.—Any contractor or awardee
10 of an agency shall immediately report to the agency
11 if the contractor or awardee has a reasonable basis
12 to conclude that—

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

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

1 “(C) the contractor or awardee has re-
2 ceived information from the agency that the
3 contractor or awardee is not authorized to re-
4 ceive in connection with the contract, grant, or
5 cooperative agreement of the contractor or
6 awardee.

7 “(2) PROCEDURES.—

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

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

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

1 **“SEC. 3596. TRAINING.**

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

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

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

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

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

22 **“SEC. 3597. ANALYSIS AND REPORT ON FEDERAL INCI-**
23 **DENTS.**

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

26 “(1) an incident, including a major incident;

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

4 “(3) a vulnerability disclosure; or

5 “(4) any other event that the Director of the
6 Cybersecurity and Infrastructure Security Agency
7 determines identifies an exploitable vulnerability in
8 an agency system.

9 “(b) ANALYSIS OF FEDERAL INCIDENTS.—

10 “(1) IN GENERAL.—The Director of the Cyber-
11 security and Infrastructure Security Agency shall
12 perform continuous monitoring of compromises of
13 agencies.

14 “(2) QUANTITATIVE AND QUALITATIVE ANAL-
15 YSES.—The Director of the Cybersecurity and Infra-
16 structure Security Agency shall develop, in consulta-
17 tion with the Director and the National Cyber Direc-
18 tor, and perform continuous monitoring and quan-
19 titative and qualitative analyses of compromises of
20 agencies, including—

21 “(A) the causes of successful compromises,
22 including—

23 “(i) attacker tactics, techniques, and
24 procedures; and

1 “(ii) system vulnerabilities, including
2 zero days, unpatched systems, and infor-
3 mation system misconfigurations;

4 “(B) the scope and scale of compromises of
5 agencies;

6 “(C) cross Federal Government root causes
7 of compromises at agencies;

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

11 “(E) lessons learned and recommendations
12 in responding to, recovering from, remediating,
13 and mitigating future incidents.

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

18 “(4) SHARING OF DATA AND ANALYSIS.—

19 “(A) IN GENERAL.—The Director shall
20 share on an ongoing basis the analyses required
21 under this subsection with agencies and the Na-
22 tional Cyber Director to—

23 “(i) improve the understanding of cy-
24 bersecurity risk of agencies; and

1 “(ii) support the cybersecurity im-
2 provement efforts of agencies.

3 “(B) FORMAT.—In carrying out subpara-
4 graph (A), the Director shall share the anal-
5 yses—

6 “(i) in human-readable written prod-
7 ucts; and

8 “(ii) to the greatest extent practicable,
9 in machine-readable formats in order to
10 enable automated intake and use by agen-
11 cies.

12 “(c) ANNUAL REPORT ON FEDERAL COM-
13 PROMISES.—Not later than 2 years after the date of en-
14 actment of this section, and not less frequently than annu-
15 ally thereafter, the Director of the Cybersecurity and In-
16 frastructure Security Agency, in consultation with the Di-
17 rector and other Federal agencies as appropriate, shall
18 submit to the appropriate notification entities a report
19 that includes—

20 “(1) a summary of causes of compromises from
21 across the Federal Government that categorizes
22 those compromises by the items described in para-
23 graphs (1) through (4) of subsection (a);

24 “(2) the quantitative and qualitative analyses of
25 compromises developed under subsection (b)(2), in-

1 including specific analysis of breaches, on an agency-
2 by-agency basis and comprehensively across the Fed-
3 eral Government; and

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

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

6 “(B) the total number of compromises of
7 the agency; and

8 “(C) a categorization of compromises of
9 the agency by the items described in para-
10 graphs (1) through (4) of subsection (a).

11 “(d) PUBLICATION.—A version of each report sub-
12 mitted under subsection (c) shall be made publicly avail-
13 able on the website of the Cybersecurity and Infrastruc-
14 ture Security Agency during the year in which the report
15 is submitted.

16 “(e) INFORMATION PROVIDED BY AGENCIES.—

17 “(1) IN GENERAL.—The analysis required
18 under subsection (b) and each report submitted
19 under subsection (c) shall use information provided
20 by agencies under section 3594(a).

21 “(2) NONCOMPLIANCE REPORTS.—

22 “(A) IN GENERAL.—Subject to subpara-
23 graph (B), during any year during which the
24 head of an agency does not provide data for an
25 incident to the Cybersecurity and Infrastructure

1 Security Agency in accordance with section
2 3594(a), the head of the agency, in coordina-
3 tion with the Director of the Cybersecurity and
4 Infrastructure Security Agency and the Direc-
5 tor, shall submit to the appropriate reporting
6 entities a report that includes—

7 “(i) data for the incident; and

8 “(ii) the information described in sub-
9 section (c) with respect to the agency.

10 “(B) EXCEPTION FOR NATIONAL SECURITY
11 SYSTEMS.—The head of an agency that owns or
12 exercises control of a national security system
13 shall not include data for an incident that oc-
14 curs on a national security system in any report
15 submitted under subparagraph (A).

16 “(3) NATIONAL SECURITY SYSTEM REPORTS.—

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

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

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

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

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

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

12 “(vi) the Committee on Oversight and
13 Reform of the House of Representatives;

14 “(vii) the Committee on Homeland
15 Security of the House of Representatives;

16 “(viii) the Permanent Select Com-
17 mittee on Intelligence of the House of Rep-
18 resentatives; and

19 “(ix) the Committee on Armed Serv-
20 ices of the House of Representatives.

21 “(B) CLASSIFIED FORM.—A report re-
22 quired under subparagraph (A) may be sub-
23 mitted in a classified form.

24 “(f) REQUIREMENT FOR COMPILING INFORMA-
25 TION.—In publishing the public report required under

1 subsection (d), the Director of the Cybersecurity and In-
2 frastructure Security Agency shall sufficiently compile in-
3 formation such that no specific incidents of an agency can
4 be identified, except with the concurrence of the Director
5 of the Office of Management and Budget and in consulta-
6 tion with the impacted agency.

7 **“SEC. 3598. MAJOR INCIDENT DEFINITION.**

8 “(a) IN GENERAL.—Not later than 180 days after
9 the date of enactment of the Federal Information Security
10 Management Act of 2021, the Director, in coordination
11 with the Director of the Cybersecurity and Infrastructure
12 Security Agency and the National Cyber Director, shall
13 develop and promulgate guidance on the definition of the
14 term ‘major incident’ for the purposes of subchapter II
15 and this subchapter.

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

19 “(1) include, with respect to any information
20 collected or maintained by or on behalf of an agency
21 or an information system used or operated by an
22 agency or by a contractor of an agency or another
23 organization on behalf of an agency—

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

1 “(i) the national security, homeland
2 security, or economic security of the
3 United States; or

4 “(ii) the civil liberties, public health
5 and safety, or individual privacy of the
6 people of the United States;

7 “(B) any incident the head of the agency
8 determines likely to result in an inability for the
9 agency, a component of the agency, or the Fed-
10 eral Government, to provide 1 or more critical
11 services;

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

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

22 “(E) any incident the head of the agency
23 determines impacts the operations of a high
24 value asset owned or operated by the agency;

1 “(F) any incident involving the exposure of
2 sensitive agency information to a foreign entity,
3 such as the communications of the head of the
4 agency, the head of a component of the agency,
5 or the direct reports of the head of the agency
6 or the head of a component of the agency; and

7 “(G) any other type of incident determined
8 appropriate by the Director;

9 “(2) stipulate that the Director shall declare a
10 major incident at each agency impacted by an inci-
11 dent if the Director of the Cybersecurity and Infra-
12 structure Security Agency determines that an inci-
13 dent—

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

15 “(B) is enabled by a common technical
16 root cause, such as a supply chain compromise,
17 a common software or hardware vulnerability;
18 or

19 “(C) is enabled by the related activities of
20 a common threat actor; and

21 “(3) stipulate that, in determining whether an
22 incident constitutes a major incident because that
23 incident—

24 “(A) is any incident described in para-
25 graph (1), the head of an agency shall consult

1 with the Director of the Cybersecurity and In-
2 frastructure Security Agency;

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

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

9 “(i) the Privacy and Civil Liberties
10 Oversight Board; and

11 “(ii) the Executive Director of the
12 Federal Trade Commission.

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

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

1 substantial harm, physical harm, embarrassment, or
2 unfairness to an individual.

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

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

8 “(B) consider—

9 “(i) any personally identifiable infor-
10 mation that was exposed as a result of an
11 incident;

12 “(ii) the circumstances under which
13 the exposure of personally identifiable in-
14 formation of an individual occurred; and

15 “(iii) whether an independent evalua-
16 tion of the information affected by an inci-
17 dent determines that the information is
18 unreadable, including, as appropriate, in-
19 stances in which the information is—

20 “(I) encrypted; and

21 “(II) determined by the Director
22 of the Cybersecurity and Infrastruc-
23 ture Security Agency to be of suffi-
24 ciently low risk of exposure.

25 “(3) APPROVAL.—

1 “(A) IN GENERAL.—The guidance issued
2 under paragraph (1) shall include a process by
3 which the Director, jointly with the Director of
4 the Cybersecurity and Infrastructure Security
5 Agency and the Attorney General, may approve
6 the designation of an incident that would be
7 considered high risk as lower risk if information
8 exposed by the incident is unreadable, as de-
9 scribed in paragraph (2)(B)(iii).

10 “(B) DOCUMENTATION.—The Director
11 shall report any approval of an incident granted
12 by the Director under subparagraph (A) to—

13 “(i) the head of the agency that expe-
14 rienced the incident;

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

17 “(iii) the Director of the Cybersecu-
18 rity and Infrastructure Security Agency.

19 “(d) EVALUATION AND UPDATES.—Not later than 2
20 years after the date of enactment of the Federal Informa-
21 tion Security Modernization Act of 2021, and not less fre-
22 quently than every 2 years thereafter, the Director shall
23 submit to the Committee on Homeland Security and Gov-
24 ernmental Affairs of the Senate and the Committee on

1 Oversight and Reform of the House of Representatives an
 2 evaluation, which shall include—

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

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

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

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

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

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification of breach.

“3593. Congressional and Executive Branch reports.

“3594. Government information sharing and incident response.

“3595. Responsibilities of contractors and awardees.

“3596. Training.

“3597. Analysis and report on Federal incidents.

“3598. Major incident definition.”.

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

17 (a) INFORMATION TECHNOLOGY MODERNIZATION
 18 CENTERS OF EXCELLENCE PROGRAM ACT.—Section
 19 2(c)(4)(A)(ii) of the Information Technology Moderniza-
 20 tion Centers of Excellence Program Act (40 U.S.C. 11301
 21 note) is amended by striking the period at the end and

1 inserting “, which shall be provided in coordination with
2 the Director of the Cybersecurity and Infrastructure Secu-
3 rity Agency.”.

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

8 (1) in section 1077(b)—

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

12 (B) in paragraph (7)—

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

15 (ii) by striking “In evaluating
16 projects” and inserting the following:

17 “(A) CONSIDERATION OF GUIDANCE.—In
18 evaluating projects”;

19 (iii) in subparagraph (A), as so des-
20 ignated, by striking “under section
21 1094(b)(1)” and inserting “guidance
22 issued by the Director”; and

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

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

9 (2) in section 1078—

10 (A) by striking subsection (a) and insert-
11 ing the following:

12 “(a) DEFINITIONS.—In this section:

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

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

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

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

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

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

7 (C) in subsection (c)—

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

12 (ii) in paragraph (5)—

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

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

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

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

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

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

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

7 “(iii) The Director shall provide to the
8 National Cyber Director any cybersecurity
9 funding information described in subpara-
10 graph (A)(ii) provided to the Director
11 under clause (ii).”; and

12 (III) in subparagraph (B), in the
13 matter preceding clause (i), by insert-
14 ing “not later than 30 days after the
15 date on which the review under sub-
16 paragraph (A) is completed,” before
17 “the Administrator”;

18 (C) in subsection (f)—

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

22 “(1) develop”;

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

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

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

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

10 (2) in section 11303(b)—

11 (A) in paragraph (2)(B)—

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

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

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

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

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

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

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

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

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

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

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

17 “(2) the head of the component agency.”.(4) in
18 section 11317, by inserting ‘security,’ before “or
19 schedule”; and

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

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

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

3 (2) in subsection (b)(1)(A)—

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

6 (B) by striking “the Secretary of Home-
7 land Security” and inserting “the Director of
8 the Cybersecurity and Infrastructure Security
9 Agency”; and

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

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

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

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

1 standards made compulsory and binding by the
2 Director; and

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

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

12 “(A) the status of cybersecurity remedial
13 actions of the agency;

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

16 “(C) incident information of the agency;

17 “(D) information from—

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

20 “(ii) information from the verification
21 disclosure program established under sec-
22 tion 3559B of title 44;

23 “(E) agency threat hunting results under
24 section 207 of the Federal Information Security
25 Modernization Act of 2021;

1 “(F) Federal and non-Federal threat intel-
2 ligence;

3 “(G) data on compliance to standards
4 issued under this section;

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

8 “(I) any other information determined rel-
9 evant by the head of the agency.”;
10 (4) in subsection (d)(2)—

11 (A) by striking the paragraph heading and
12 inserting CONSULTATION, NOTICE, AND
13 COMMENT;

14 (B) by inserting “promulgate,” before
15 “significantly modify”; and

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

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

24 “(B) in consultation with the Chief Infor-
25 mation Officers Council, the Director of the Cy-

1 bersecurity and Infrastructure Security Agency,
2 the National Cyber Director, the Comptroller
3 General of the United States, and the Council
4 of the Inspectors General on Integrity and Effi-
5 ciency;

6 “(C) considering the Federal risk assess-
7 ments performed under section 3553(i) of title
8 44; and

9 “(D) considering the extent to which the
10 proposed standard reduces risk relative to the
11 cost of implementation of the standard.”; and

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

13 “(e) REVIEW OF OFFICE OF MANAGEMENT AND
14 BUDGET GUIDANCE AND POLICY.—

15 “(1) IN GENERAL.—Not less frequently than
16 once every 3 years, the Director of the Office of
17 Management and Budget, in consultation with the
18 Chief Information Officers Council, the Director of
19 the Cybersecurity and Infrastructure Security Agen-
20 cy, the National Cyber Director, the Comptroller
21 General of the United States, and the Council of the
22 Inspectors General on Integrity and Efficiency shall
23 review the efficacy of the guidance and policy pro-
24 mulgated by the Director in reducing cybersecurity
25 risks, including an assessment of the requirements

1 on agencies to report information to the Director,
2 and determine whether any changes to that guidance
3 or policy is appropriate.

4 “(A) The Director shall consider the Fed-
5 eral risk assessment developed under section
6 3553(i) of title 44 as part of the review

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

13 “(3) PUBLIC REPORT.—Not later than 30 days
14 after the date of the completion of the review under
15 paragraph (1), the Director of the Office of Manage-
16 ment and Budget shall publicly publish a report that
17 includes—

18 “(A) an overview of the guidance and pol-
19 icy currently in effect promulgated under this
20 section;

21 “(B) the cybersecurity risk mitigation, or
22 other cybersecurity benefit, offered by each
23 guidance or policy document described in sub-
24 paragraph (A); and

1 “(C) a summary of the guidance or policy
2 to which changes were determined appropriate
3 during the review and what the changes are an-
4 ticipated to include; and

5 “(4) CONGRESSIONAL BRIEFING.—Not later
6 than 30 days after the date on which a review is
7 completed under paragraph (1), the Director shall
8 provide to the Committee on Homeland Security and
9 Governmental Affairs of the Senate and the Com-
10 mittee on Oversight and Reform of the House of
11 Representatives a briefing on the review completed
12 pursuant to (1).

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

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

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

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

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

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

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

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

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

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

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

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

8 (1) FISMA.—Section 2 of the Federal Informa-
9 tion Security Modernization Act of 2014 (44 U.S.C.
10 3554 note) is amended—

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

12 (B) by redesignating subsections (c)
13 through (f) as subsections (b) through (e), re-
14 spectively.

15 (2) INCIDENT DATA SHARING.—

16 (A) IN GENERAL.—The Director shall de-
17 velop guidance, to be updated not less fre-
18 quently than once every 2 years, on the content,
19 timeliness, and format of the information pro-
20 vided by agencies under section 3594(a) of title
21 44, United States Code, as added by this Act.

22 (B) REQUIREMENTS.—The guidance devel-
23 oped under subparagraph (A) shall—

24 (i) prioritize the availability of data
25 necessary to understand and analyze—

84

- 1 (I) the causes of incidents;
- 2 (II) the scope and scale of inci-
- 3 dents within the environments and
- 4 systems of an agency;
- 5 (III) a root cause analysis of in-
- 6 cidents that—
- 7 (aa) are common across the
- 8 Federal Government; or
- 9 (bb) have a Government-
- 10 wide impact;
- 11 (IV) agency response, recovery,
- 12 and remediation actions and the effec-
- 13 tiveness of those actions; and
- 14 (V) the impact of incidents;
- 15 (ii) enable the efficient development
- 16 of—
- 17 (I) lessons learned and rec-
- 18 ommendations in responding to, recov-
- 19 ering from, remediating, and miti-
- 20 gating future incidents; and
- 21 (II) the report on Federal com-
- 22 promises required under section
- 23 3597(e) of title 44, United States
- 24 Code, as added by this Act;

1 (iii) include requirements for the time-
2 liness of data production; and

3 (iv) include requirements for using
4 automation and machine-readable data for
5 data sharing and availability.

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

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

23 (5) CONTRACTOR AND GRANTEE GUIDANCE.—

24 (A) IN GENERAL.—Not later than 1 year
25 after the date of enactment of this Act, the Di-

1 rector, in coordination with the Secretary of
2 Homeland Security, the Secretary of Defense,
3 the Administrator of General Services, and the
4 heads of other agencies determined appropriate
5 by the Director, shall issue guidance to Federal
6 agencies on how to deconflict, to the greatest
7 extent practicable, existing regulations, policies,
8 and procedures relating to the responsibilities of
9 contractors and awardees established under sec-
10 tion 3595 of title 44, United States Code, as
11 added by this Act.

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

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

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

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

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

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

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

14 **SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**
15 **UPDATES.**

16 Not later than 1 year after the date of enactment
17 of this Act, the Director, in coordination with the Director
18 of the Cybersecurity and Infrastructure Security Agency,
19 shall issue guidance for agencies on—

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

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

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

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

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

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

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

22 (6) requiring, as practical and pursuant to sec-
23 tion 203, an evaluation of agency cybersecurity
24 using metrics that are—

25 (A) based on outcomes; and

1 (B) based on time.

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

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

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

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

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

16 **SEC. 201. EVALUATION OF EFFECTIVENESS OF IMPLE-**
17 **MENTING STANDARDS.**

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

23 (1) assesses the implementation of standards
24 promulgated under section 11331(b) of title 40,
25 United States Code, to determine the degree to

1 which agencies use the authority under subsection
2 (c)(1) of section 11331 of title 40, United States
3 Code, as amended by section 102, to customize the
4 standards relative to the risks facing each agency
5 and agency system;

6 (2) assesses the effectiveness of the implemen-
7 tation by agencies of the standards described in
8 paragraph (1), including any standards customized
9 by agencies under subsection (c)(1) of section 11331
10 of title 40, United States Code, as amended by sec-
11 tion 102, in improving agency cybersecurity;

12 (3) examines the quantification of cybersecurity
13 risk in the private sector for any applicability for use
14 by the Federal Government;

15 (4) examines cybersecurity metrics existing as
16 of the date of enactment of this Act used by the Di-
17 rector, the Director of the Cybersecurity and Infra-
18 structure Security Agency, and the heads of other
19 agencies to evaluate the effectiveness of information
20 security policies and practices; and

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

23 (A) the addition or removal of standards;

24 or

25 (B) the customization of—

1 (i) the standards by agencies under
2 subsection (c)(1) of section 11331 of title
3 40, United States Code, as amended by
4 section 102; or

5 (ii) specific controls within the stand-
6 ards.

7 (b) INCORPORATION OF STUDY.—The Director shall
8 incorporate the results of the study performed under sub-
9 section (a) into the review of guidance and policy required
10 under subsection (e) of section 11331 of title 40, United
11 States Code, as added by section 102(e) of this Act.

12 (c) BRIEFING.—Not later than 30 days after the date
13 on which the study performed under subsection (a) is com-
14 pleted, the Comptroller General of the United States shall
15 provide to the appropriate congressional committees a
16 briefing on the study.

17 **SEC. 202. MOBILE SECURITY STANDARDS.**

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

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

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

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

1 (1) a requirement, pursuant to section
2 3506(b)(4) of title 44, United States Code, for every
3 agency to maintain a continuous inventory of
4 every—

5 (A) mobile device operated by or on behalf
6 of the agency; and

7 (B) vulnerability identified by the agency
8 associated with a mobile device; and

9 (2) a requirement for every agency to perform
10 continuous evaluation of the vulnerabilities described
11 in paragraph (1)(B) and other risks associated with
12 the use of applications on mobile devices.

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

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

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

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

4 (a) ESTABLISHING TIME-BASED METRICS.—

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

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

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

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

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

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

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

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

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

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

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

11 (b) IMPLEMENTATION.—

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

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

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

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

6 (A) stores agency metrics information; and

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

10 (c) UPDATED METRICS.—

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

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

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

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

25 (d) CONGRESSIONAL REPORTS.—

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

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

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

17 (a) RECOMMENDATIONS.—Not later than 2 years
18 after the date of enactment of this Act, and not less fre-
19 quently than every 2 years thereafter, the Director of the
20 Cybersecurity and Infrastructure Security Agency, in con-
21 sultation with the Attorney General, shall submit to the
22 Director recommendations on requirements for logging
23 events on agency systems and retaining other relevant
24 data within the systems and networks of an agency.

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

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

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

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

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

10 (5) requirements to ensure that, upon request,
11 in a manner that excludes or otherwise reasonably
12 protects personally identifiable information, and to
13 the extent permitted by applicable law (including
14 privacy and statistical laws), agencies provide logs
15 to—

16 (A) the Director of the Cybersecurity and
17 Infrastructure Security Agency for a cybersecu-
18 rity purpose; and

19 (B) the Federal Bureau of Investigation to
20 investigate potential criminal activity; and

21 (6) requirements to ensure that, subject to com-
22 pliance with statistical laws and other relevant data
23 protection requirements, the highest level security
24 operations center of each agency has visibility into
25 all agency logs.

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

11 **SEC. 205. CISA AGENCY ADVISORS.**

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

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

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

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

25 (3) other Federal cybersecurity initiatives.

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

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

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

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

12 (4) other duties, as assigned.

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

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

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

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

22 **“§ 3559A. Federal penetration testing**

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

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

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

8 “(b) GUIDANCE.—

9 “(1) IN GENERAL.—Not later than 180 days
10 after the date of enactment of this section, the Di-
11 rector shall issue guidance that—

12 “(A) requires agencies to use, when and
13 where appropriate, penetration testing on agen-
14 cy systems; and

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

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

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

23 “(i) a shared service of the agency or
24 another agency; or

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

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

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

12 “(1) require the agency to—

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

15 “(B) coordinate with the Director of the
16 Cybersecurity and Infrastructure Security agen-
17 cy to ensure that penetration testing is being
18 performed;

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

21 “(A) adverse impacts to the operations of
22 the agency;

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

25 “(C) inappropriate access to data;

1 “(3) require the results of penetration testing
2 to include feedback to improve the cybersecurity of
3 the agency; and

4 “(4) include mechanisms for providing consist-
5 ently formatted, and, if applicable, automated and
6 machine-readable, data to the Director and the Di-
7 rector of the Cybersecurity and Infrastructure Secu-
8 rity Agency.

9 “(d) RESPONSIBILITIES OF CISA.—The Director of
10 the Cybersecurity and Infrastructure Security Agency
11 shall—

12 “(1) establish a process to assess the perform-
13 ance of penetration testing by both Federal and non-
14 Federal entities that establishes minimum quality
15 controls for penetration testing;

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

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

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

23 “(e) RESPONSIBILITIES OF OMB.—The Director, in
24 coordination with the Director of the Cybersecurity and
25 Infrastructure Security Agency, shall—

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

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

5 “(f) PRIORITIZATION OF PENETRATION TESTING RE-
6 SOURCES.—

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

12 “(2) CONSIDERATIONS.—In developing the
13 framework under this subsection, the Director shall
14 consider—

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

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

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

21 “(D) any other information determined ap-
22 propriate by the Director or the Director of the
23 Cybersecurity and Infrastructure Security
24 Agency.

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

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

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

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

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

 “3559A. Federal penetration testing.”.

15 (c) PENETRATION TESTING BY THE SECRETARY OF
16 HOMELAND SECURITY.—Section 3553(b) of title 44,
17 United States Code, as amended by section 101, is further
18 amended—

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

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

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

1 “(9) performing penetration testing with or
2 without advance notice to, or authorization from,
3 agencies, to identify vulnerabilities within Federal
4 information systems; and”.

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

6 (a) **THREAT HUNTING PROGRAM.—**

7 (1) **IN GENERAL.—**Not later than 540 days
8 after the date of enactment of this Act, the Director
9 of the Cybersecurity and Infrastructure Security
10 Agency shall establish a program to provide ongoing,
11 hypothesis-driven threat-hunting services on the net-
12 work of each agency.

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

20 (A) determine the method for collecting,
21 storing, accessing, and analyzing appropriate
22 agency data;

23 (B) provide on-premises support to agen-
24 cies;

25 (C) staff threat hunting services;

1 (D) allocate available human and financial
2 resources to implement the plan; and

3 (E) provide input to the heads of agencies
4 on the use of—

5 (i) more stringent standards under
6 section 11331(c)(1) of title 40, United
7 States Code; and

8 (ii) additional cybersecurity proce-
9 dures under section 3554 of title 44,
10 United States Code.

11 (b) REPORTS.—The Director of the Cybersecurity
12 and Infrastructure Security Agency shall submit to the ap-
13 propriate congressional committees—

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

19 (2) not less than 30 days before the date on
20 which the Director of the Cybersecurity and Infra-
21 structure Security Agency begins providing threat
22 hunting services under the program under sub-
23 section (a)(1), a report providing any updates to the
24 plan developed under subsection (a)(2); and

1 (3) not later than 1 year after the date on
2 which the Director of the Cybersecurity and Infra-
3 structure Security Agency begins providing threat
4 hunting services to agencies other than the Cyberse-
5 curity and Infrastructure Security Agency, a report
6 describing lessons learned from providing those serv-
7 ices.

8 **SEC. 208. CODIFYING VULNERABILITY DISCLOSURE PRO-**
9 **GRAMS.**

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

13 **“§ 3559B. Federal vulnerability disclosure programs**

14 “(a) DEFINITIONS.—In this section:

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

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

22 “(b) RESPONSIBILITIES OF OMB.—

23 “(1) LIMITATION ON LEGAL ACTION.—The Di-
24 rector, in consultation with the Attorney General,
25 shall issue guidance to agencies to not recommend or

1 pursue legal action against a reporter or an indi-
2 vidual that conducts a security research activity that
3 the head of the agency determines—

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

7 “(B) is authorized under the vulnerability
8 disclosure policy of the agency developed under
9 subsection (d)(2).

10 “(2) SHARING INFORMATION WITH CISA.—The
11 Director, in coordination with the Director of the
12 Cybersecurity and Infrastructure Security Agency,
13 shall issue guidance to agencies on sharing relevant
14 information in a consistent, automated, and machine
15 readable manner with the Cybersecurity and Infra-
16 structure Security Agency, including—

17 “(A) any valid or credible reports of newly
18 discovered or not publicly known vulnerabilities
19 (including misconfigurations) on Federal infor-
20 mation systems that use commercial software or
21 services;

22 “(B) information relating to vulnerability
23 disclosure, coordination, or remediation activi-
24 ties of an agency, particularly as those activities
25 relate to outside organizations—

1 “(i) with which the head of the agency
2 believes the Director of the Cybersecurity
3 and Infrastructure Security Agency can as-
4 sist; or

5 “(ii) about which the head of the
6 agency believes the Director of the Cyber-
7 security and Infrastructure Security Agen-
8 cy should know; and

9 “(C) any other information with respect to
10 which the head of the agency determines helpful
11 or necessary to involve the Cybersecurity and
12 Infrastructure Security Agency.

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

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

21 “(1) provide support to agencies with respect to
22 the implementation of the requirements of this sec-
23 tion;

24 “(2) develop tools, processes, and other mecha-
25 nisms determined appropriate to offer agencies capa-

1 bilities to implement the requirements of this sec-
2 tion; and

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

6 “(d) RESPONSIBILITIES OF AGENCIES.—

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

11 “(A) an appropriate security contact; and

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

15 “(2) VULNERABILITY DISCLOSURE POLICY.—

16 The head of each agency shall develop and make
17 publicly available a vulnerability disclosure policy for
18 the agency, which shall—

19 “(A) describe—

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

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

1 “(iii) the type of information system
2 testing that is not authorized by the agen-
3 cy; and

4 “(iv) the disclosure policy of the agen-
5 cy for sensitive information;

6 “(B) with respect to a report to an agency,
7 describe—

8 “(i) how the reporter should submit
9 the report; and

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

14 “(C) include any other relevant informa-
15 tion; and

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

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

24 “(e) PAPERWORK REDUCTION ACT EXEMPTION.—

25 The requirements of subchapter I (commonly known as

1 the ‘Paperwork Reduction Act’) shall not apply to a vul-
2 nerability disclosure program established under this sec-
3 tion.

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

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

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

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

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

4 (b) CLERICAL AMENDMENT.—The table of sections
5 for chapter 35 of title 44, United States Code, is amended
6 by adding after the item relating to section 3559A, as
7 added by section 206, the following:

 “3559B. Federal vulnerability disclosure programs.”.

8 **SEC. 209. IMPLEMENTING PRESUMPTION OF COMPROMISE**
9 **AND ZERO TRUST ARCHITECTURES.**

10 (a) GUIDANCE.—Not later than 180 days after the
11 date of enactment of this Act, the Director, in consultation
12 with the Director of the Cybersecurity and Infrastructure
13 Security Agency and the Director of the National Institute
14 of Standards and Technology, shall issue guidance to
15 agencies to increase the security of agency systems to by
16 utilizing presumption of compromise and least privilege
17 principles.

18 (b) AGENCY IMPLEMENTATION PLANS.—Not later
19 than 60 days after the date on which the Director issues
20 guidance under subsection (a), the head of each agency
21 shall submit to the Director a plan to implement the guid-
22 ance, which shall include—

23 (1) a description of any steps the agency has
24 completed;

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

3 (3) a schedule to implement the plan.

4 (c) REPORT AND BRIEFING.—Not later than 90 days
5 after the date on which the Director issues guidance re-
6 quired under subsection (a), the Director shall provide a
7 briefing to the appropriate congressional committees on
8 the guidance and the agency implementation plans sub-
9 mitted under subsection (b).

10 **SEC. 210. AUTOMATION REPORTS.**

11 (a) OMB REPORT.—Not later than 180 days after
12 the date of enactment of this Act, the Director shall report
13 to the appropriate congressional committees on the use of
14 automation under paragraphs (1), (5)(C) and (8)(B) of
15 section 3554(b) of title 44, United States Code.

16 (b) GAO REPORT.—Not later than 1 year after the
17 date of enactment of this Act, the Comptroller General
18 of the United States shall perform a study on the use of
19 automation and machine readable data across the Federal
20 Government for cybersecurity purposes, including the
21 automated updating of cybersecurity tools, sensors, or
22 processes by agencies.

1 **SEC. 211. EXTENSION OF FEDERAL ACQUISITION SECURITY**

2 **COUNCIL.**

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

6 **SEC. 212. COUNCIL OF THE INSPECTORS GENERAL ON IN-**

7 **TEGRITY AND EFFICIENCY DASHBOARD.**

8 (a) **DASHBOARD REQUIRED.**—Section 11(e)(2) of the
9 Inspector General Act of 1978 (5 U.S.C. App.) is amend-
10 ed—

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

13 (2) by redesignating subparagraph (B) as sub-
14 paragraph (C); and

15 (3) by inserting after subparagraph (A) the fol-
16 lowing:

17 “(B) that shall include a dashboard of
18 open information security recommendations
19 identified in the independent evaluations re-
20 quired by section 3555(a) of title 44, United
21 States Code; and”.

22 **SEC. 213. NATIONAL SECURITY AND DEPARTMENT OF DE-**

23 **FENSE SYSTEMS.**

24 (a) **NATIONAL SECURITY SYSTEMS.**—The authorities
25 and functions of the Director and the Director of the Cy-

1 bersecurity and Infrastructure Security Agency under this
2 title shall not apply to national security systems.

3 (b) DELEGATION OF AUTHORITIES.—The authorities
4 of the Director and the Director of the Cybersecurity and
5 Infrastructure Security Agency described in this title shall
6 be delegated—

7 (1) to the Secretary of Defense in the case of
8 systems described in section 3553(e)(2) of title 44,
9 United States Code; and

10 (2) to the Director of National Intelligence in
11 the case of systems described in section 3553(e)(3)
12 of title 44, United States Code.

13 **TITLE III—RISK-BASED BUDGET** 14 **MODEL**

15 **SEC. 301. DEFINITIONS.**

16 In this title:

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

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

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

1 (2) COVERED AGENCY.—The term “covered
2 agency” has the meaning given the term “executive
3 agency” in section 133 of title 41, United States
4 Code.

5 (3) DIRECTOR.—The term “Director” means
6 the Director of the Office of Management and Budg-
7 et.

8 (4) INFORMATION TECHNOLOGY.—The term
9 “information technology”—

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

12 (B) includes the hardware and software
13 systems of a Federal agency that monitor and
14 control physical equipment and processes of the
15 Federal agency.

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

18 (A) developed by identifying and
19 prioritizing cybersecurity risks and
20 vulnerabilities, including impact on agency oper-
21 ations in the case of a cyber attack, through
22 analysis of threat intelligence, incident data,
23 and tactics, techniques, procedures, and capa-
24 bilities of cyber threats; and

1 (B) that allocates resources based on the
2 risks identified and prioritized under subpara-
3 graph (A).

4 **SEC. 302. ESTABLISHMENT OF RISK-BASED BUDGET**
5 **MODEL.**

6 (a) IN GENERAL.—

7 (1) MODEL.—Not later than 1 year after the
8 first publication of the budget submitted by the
9 President under section 1105 of title 31, United
10 States Code, following the date of enactment of this
11 Act, the Director, in consultation with the Director
12 of the Cybersecurity and Infrastructure Security
13 Agency and the National Cyber Director and in co-
14 ordination with the Director of the National Insti-
15 tute of Standards and Technology, shall develop a
16 standard model for creating a risk-based budget for
17 cybersecurity spending.

18 (2) RESPONSIBILITY OF DIRECTOR.—Section
19 3553(a) of title 44, United States Code, as amended
20 by section 101, is further amended by inserting after
21 paragraph (6) the following:

22 “(7) developing a standard risk-based budget
23 model to inform Federal agency cybersecurity budget
24 development; and”.

1 (E) be used to evaluate and inform govern-
2 ment-wide cybersecurity programs of the De-
3 partment of Homeland Security.

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

8 (5) PUBLICATION.—The Director shall publish
9 the model required to be developed under this sub-
10 section, and any updates necessary under paragraph
11 (4), on the public website of the Office of Manage-
12 ment and Budget.

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

20 (b) REQUIRED USE OF RISK-BASED BUDGET
21 MODEL.—

22 (1) IN GENERAL.—Not later than 2 years after
23 the date on which the model developed under sub-
24 section (a) is published, the head of each covered
25 agency shall use the model to develop the annual cy-

1 bersecurity and information technology budget re-
2 quests of the agency.

3 (2) AGENCY PERFORMANCE PLANS.—Section
4 3554(d)(2) of title 44, United States Code, is
5 amended by inserting “and the risk-based budget
6 model required under section 3553(a)(7)” after
7 “paragraph (1)”.

8 (c) VERIFICATION.—

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

11 (A) in the matter preceding subclause (I),
12 by striking “by agency, and by initiative area
13 (as determined by the administration)” and in-
14 serting “and by agency”;

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

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

18 “(V) a validation that the budg-
19 ets submitted were developed using a
20 risk-based methodology; and

21 “(VI) a report on the progress of
22 each agency on closing recommenda-
23 tions identified under the independent
24 evaluation required by section
25 3555(a)(1) of title 44.”.

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

5 (d) ANNUAL REPORTS.—

6 (1) ANNUAL INDEPENDENT EVALUATION.—Sec-
7 tion 3555(a)(2) of title 44, United States Code, is
8 amended—

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

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

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

14 “(D) an assessment of how the agency im-
15 plemented the risk-based budget model required
16 under section 3553(a)(7) and an evaluation of
17 whether the model mitigates agency cyber
18 vulnerabilities.”.

19 (2) ASSESSMENT.—Section 3553(c) of title 44,
20 United States Code, as amended by section 101, is
21 further amended by inserting after paragraph (5)
22 the following:

23 “(6) an assessment of—

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

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

3 “(C) whether the model mitigates the
4 cyber vulnerabilities of the Federal Government;
5 and”.

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

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

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

18 (3) an evaluation of whether the risk-based
19 budgets developed by covered agencies mitigate
20 cyber vulnerability, including the extent to which the
21 risk-based budgets inform Federal Government-wide
22 cybersecurity programs; and

23 (4) any other information relating to risk-based
24 budgets the Comptroller General determines appro-
25 priate.

1 **TITLE IV—PILOT PROGRAMS TO**
2 **ENHANCE FEDERAL CYBER-**
3 **SECURITY**

4 **SEC. 401. CONTINUOUS INDEPENDENT EVALUATION PILOT.**

5 (a) IN GENERAL.—Not later than 2 years after the
6 date of enactment of this Act, the Director, in coordina-
7 tion with the Director of the Cybersecurity and Infrastruc-
8 ture Security Agency, shall establish a pilot program to
9 perform continual agency evaluation of the cybersecurity
10 of the agency.

11 (b) PURPOSE.—

12 (1) IN GENERAL.—The purpose of the pilot
13 program established under subsection (a) shall be to
14 develop the capability to continuously evaluate agen-
15 cy cybersecurity postures, rather than performing an
16 annual evaluation.

17 (2) USE OF INFORMATION.—It is the sense of
18 Congress that information relating to agency cyber-
19 security postures should be used, on an ongoing
20 basis, to increase agency understanding of cyberse-
21 curity risk and improve agency cybersecurity.

22 (c) PARTICIPATING AGENCIES.—

23 (1) IN GENERAL.—The Director, in coordina-
24 tion with the Council of the Inspectors General on
25 Integrity and Efficiency and in consultation with the

1 Director of the Cybersecurity and Infrastructure Se-
2 curity Agency, shall identify not less than 1 agency
3 and the Inspector General of each identified agency
4 to participate in the pilot program established under
5 subsection (a).

6 (2) CAPABILITIES OF AGENCY.—An agency se-
7 lected under paragraph (1) shall have advanced cy-
8 bersecurity capabilities and automated and machine-
9 readable means of sharing information.

10 (3) CAPABILITIES OF INSPECTOR GENERAL.—
11 The Inspector General of an agency selected under
12 paragraph (1) shall have advanced cybersecurity ca-
13 pabilities, including the ability—

14 (A) to utilize, when appropriate, automated
15 tools to gain insight into the cybersecurity pos-
16 ture of the agency; and

17 (B) to assess the impact and deployment
18 of additional cybersecurity procedures.

19 (d) DUTIES.—The Director, in coordination with the
20 Council of the Inspectors General on Integrity and Effi-
21 ciency, the Director of the Cybersecurity and Infrastruc-
22 ture Security Agency, and the head of each agency partici-
23 pating in the pilot program under subsection (c), shall de-
24 velop processes and procedures to perform a continuous

1 independent evaluation of the overall cybersecurity posture
2 of the agency, which may include an evaluation of—

3 (1) the status of cybersecurity remedial actions
4 of the agency;

5 (2) any vulnerability information relating to
6 agency systems that is known to the agency;

7 (3) incident information of the agency;

8 (4) penetration testing performed by an exter-
9 nal entity under section 3559A of title 44, United
10 States Code;

11 (5) information from the vulnerability disclo-
12 sure program information established under section
13 3559B of title 44, United States Code;

14 (6) agency threat hunting results; and

15 (7) any other information determined relevant
16 by the Director.

17 (e) INDEPENDENT EVALUATION WAIVER.—With re-
18 spect to an agency that participates in the pilot program
19 under subsection (a) during any year other than the first
20 year during which the pilot program is conducted, the Di-
21 rector, with the concurrence of the Director of the Cyber-
22 security and Infrastructure Security Agency, may waive
23 any requirement of the agency with respect to the annual
24 independent evaluation under section 3555 of title 44,
25 United States Code.

1 (f) DURATION.—The pilot program established under
2 this section—

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

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

18 (g) REPORTS.—

19 (1) PILOT PROGRAM PLAN.—Before identifying
20 any agencies to participate in the pilot program
21 under subsection (c), the Director, in coordination
22 with the Director of the Cybersecurity and Infra-
23 structure Security Agency and the Council of the In-
24 spectors General on Integrity and Efficiency, shall
25 submit to the appropriate congressional committees

1 a plan for the pilot program that outlines selection
2 criteria and preliminary plans to implement the pilot
3 program.

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

9 (A) the selection of agencies to participate
10 in the pilot program; and

11 (B) processes and procedures to perform a
12 continuous independent evaluation of agencies.

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

1 **SEC. 402. ACTIVE CYBER DEFENSIVE STUDY.**

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

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

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

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

18 (1) a review of legal restrictions on the use of
19 different active cyber defense techniques in Federal
20 environments, in consultation with the Department
21 of Justice;

22 (2) an evaluation of—

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

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

4 (3) recommendations on safeguards and proce-
5 dures that shall be established to require that active
6 defense techniques are adequately coordinated to en-
7 sure that active defense techniques do not impede
8 threat response efforts, criminal investigations, and
9 national security activities, including intelligence col-
10 lection; and

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

13 **SEC. 403. SECURITY OPERATIONS CENTER AS A SERVICE**
14 **PILOT.**

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

21 (b) PLAN.—Not later than 1 year after the date of
22 enactment of this Act, the Director of the Cybersecurity
23 and Infrastructure Security Agency shall develop a plan
24 to establish a centralized Federal security operations cen-

1 ter shared service offering within the Cybersecurity and
2 Infrastructure Security Agency.

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

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

7 (2) staffing and resources; and

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

10 (d) PILOT PROGRAM.—

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

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

25 (e) BRIEFING AND REPORT.—

1 (1) BRIEFING.—Not later than 260 days after
2 the date of enactment of this Act, the Director of
3 the Cybersecurity and Infrastructure Security Agen-
4 cy shall provide to the Committee on Homeland Se-
5 curity and Governmental Affairs of the Senate and
6 the Committee on Homeland Security and the Com-
7 mittee on Oversight and Reform of the House of
8 Representatives a briefing on the parameters of any
9 1-year agreements entered into under subsection
10 (d)(1).

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

20 (A) the agreement; and

21 (B) any additional agreements entered into
22 with agencies under subsection (d).