

Calendar No. 265

117TH CONGRESS
2D SESSION**S. 3600**

To improve the cybersecurity of the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 8 (legislative day, FEBRUARY 3), 2022

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill;
which was read the first time

FEBRUARY 9, 2022

Read the second time and placed on the calendar

A BILL

To improve the cybersecurity of the Federal Government,
and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Strengthening Amer-
5 ican Cybersecurity Act of 2022”.

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

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

Sec. 1. Short title.

Sec. 2. Table of contents.

TITLE I—FEDERAL INFORMATION SECURITY MODERNIZATION
ACT OF 2022

- Sec. 101. Short title.
- Sec. 102. Definitions.
- Sec. 103. Title 44 amendments.
- Sec. 104. Amendments to subtitle III of title 40.
- Sec. 105. Actions to enhance Federal incident transparency.
- Sec. 106. Additional guidance to agencies on FISMA updates.
- Sec. 107. Agency requirements to notify private sector entities impacted by incidents.
- Sec. 108. Mobile security standards.
- Sec. 109. Data and logging retention for incident response.
- Sec. 110. CISA agency advisors.
- Sec. 111. Federal penetration testing policy.
- Sec. 112. Ongoing threat hunting program.
- Sec. 113. Codifying vulnerability disclosure programs.
- Sec. 114. Implementing zero trust architecture.
- Sec. 115. Automation reports.
- Sec. 116. Extension of Federal acquisition security council and software inventory.
- Sec. 117. Council of the Inspectors General on Integrity and Efficiency dashboard.
- Sec. 118. Quantitative cybersecurity metrics.
- Sec. 119. Establishment of risk-based budget model.
- Sec. 120. Active cyber defensive study.
- Sec. 121. Security operations center as a service pilot.
- Sec. 122. Extension of Chief Data Officer Council.

TITLE II—CYBER INCIDENT REPORTING FOR CRITICAL
INFRASTRUCTURE ACT OF 2022

- Sec. 201. Short title.
- Sec. 202. Definitions.
- Sec. 203. Cyber incident reporting.
- Sec. 204. Federal sharing of incident reports.
- Sec. 205. Ransomware vulnerability warning pilot program.
- Sec. 206. Ransomware threat mitigation activities.
- Sec. 207. Congressional reporting.

TITLE III—FEDERAL SECURE CLOUD IMPROVEMENT AND JOBS
ACT OF 2022

- Sec. 301. Short title.
- Sec. 302. Findings.
- Sec. 303. Title 44 amendments.

1 **TITLE I—FEDERAL INFORMA-**
2 **TION SECURITY MODERNIZA-**
3 **TION ACT OF 2022**

4 **SEC. 101. SHORT TITLE.**

5 This title may be cited as the “Federal Information
6 Security Modernization Act of 2022”.

7 **SEC. 102. DEFINITIONS.**

8 In this title, unless otherwise specified:

9 (1) **ADDITIONAL CYBERSECURITY PROCE-**
10 **DURE.**—The term “additional cybersecurity proce-
11 dure” has the meaning given the term in section
12 3552(b) of title 44, United States Code, as amended
13 by this title.

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

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

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

22 (B) the Committee on Oversight and Re-
23 form of the House of Representatives; and

24 (C) the Committee on Homeland Security
25 of the House of Representatives.

1 (4) DIRECTOR.—The term “Director” means
2 the Director of the Office of Management and Budg-
3 et.

4 (5) INCIDENT.—The term “incident” has the
5 meaning given the term in section 3552(b) of title
6 44, United States Code.

7 (6) NATIONAL SECURITY SYSTEM.—The term
8 “national security system” has the meaning given
9 the term in section 3552(b) of title 44, United
10 States Code.

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

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

19 **SEC. 103. TITLE 44 AMENDMENTS.**

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

22 (1) in section 3504—

23 (A) in subsection (a)(1)(B)—

24 (i) by striking clause (v) and inserting
25 the following:

1 “(v) confidentiality, privacy, disclosure,
2 and sharing of information;”;

3 (ii) by redesignating clause (vi) as
4 clause (vii); and

5 (iii) by inserting after clause (v) the
6 following:

7 “(vi) in consultation with the National
8 Cyber Director, security of information; and”;
9 and

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

12 “(1) develop and oversee the implementation of
13 policies, principles, standards, and guidelines on pri-
14 vacy, confidentiality, disclosure, and sharing, and in
15 consultation with the National Cyber Director, over-
16 see the implementation of policies, principles, stand-
17 ards, and guidelines on security, of information col-
18 lected or maintained by or for agencies; and”;

19 (2) in section 3505—

20 (A) by striking the first subsection des-
21 ignated as subsection (c);

22 (B) in paragraph (2) of the second sub-
23 section designated as subsection (c), by insert-
24 ing “an identification of internet accessible in-

formation systems and” after “an inventory under this subsection shall include”;

(C) in paragraph (3) of the second subsection designated as subsection (c)—

(i) in subparagraph (B)—

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

(II) by striking “and” at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting “; and”; and

(iii) by adding at the end the following:

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

(3) in section 3506—

(A) in subsection (a)(3), by inserting “In carrying out these duties, the Chief Information Officer shall coordinate, as appropriate, with the Chief Data Officer in accordance with the designated functions under section 3520(c).”

1 after “reduction of information collection bur-
 2 dens on the public.”;

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

5 (C) in subsection (h)(3), by inserting “se-
 6 curity,” after “efficiency,”; and

7 (4) in section 3513—

8 (A) by redesignating subsection (c) as sub-
 9 section (d); and

10 (B) by inserting after subsection (b) the
 11 following:

12 “(c) Each agency providing a written plan under sub-
 13 section (b) shall provide any portion of the written plan
 14 addressing information security to the Secretary of the
 15 Department of Homeland Security and the National Cyber
 16 Director.”.

17 (b) SUBCHAPTER II DEFINITIONS.—

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

20 (A) by redesignating paragraphs (1), (2),
 21 (3), (4), (5), (6), and (7) as paragraphs (2),
 22 (4), (5), (6), (7), (9), and (11), respectively;

23 (B) by inserting before paragraph (2), as
 24 so redesignated, the following:

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

7 (C) by inserting after paragraph (2), as so
8 redesignated, the following:

9 “(3) The term ‘high value asset’ means infor-
10 mation or an information system that the head of an
11 agency, using policies, principles, standards, or
12 guidelines issued by the Director under section
13 3553(a), determines to be so critical to the agency
14 that the loss or corruption of the information or the
15 loss of access to the information system would have
16 a serious impact on the ability of the agency to per-
17 form the mission of the agency or conduct busi-
18 ness.”;

19 (D) by inserting after paragraph (7), as so
20 redesignated, the following:

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

24 (E) by inserting after paragraph (9), as so
25 redesignated, the following:

1 “(10) The term ‘penetration test’—

2 “(A) means an authorized assessment that
3 emulates attempts to gain unauthorized access
4 to, or disrupt the operations of, an information
5 system or component of an information system;
6 and

7 “(B) includes any additional meaning
8 given the term in policies, principles, standards,
9 or guidelines issued by the Director under sec-
10 tion 3553(a).”; and

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

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

17 (2) CONFORMING AMENDMENTS.—

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

23 (B) TITLE 10.—

24 (i) SECTION 2222.—Section 2222(i)(8)
25 of title 10, United States Code, is amended

by striking “section 3552(b)(6)(A)” and
inserting “section 3552(b)(9)(A)”.

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

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

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

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

(D) INTERNET OF THINGS CYBERSECURITY
IMPROVEMENT ACT OF 2020.—Section 3(5)
of the Internet of Things Cybersecurity Im-

1 provement Act of 2020 (15 U.S.C. 278g–3a) is
 2 amended by striking “section 3552(b)(6)” and
 3 inserting “section 3552(b)”.

4 (E) NATIONAL DEFENSE AUTHORIZATION
 5 ACT FOR FISCAL YEAR 2013.—Section
 6 933(e)(1)(B) of the National Defense Author-
 7 ization Act for Fiscal Year 2013 (10 U.S.C.
 8 2224 note) is amended by striking “section
 9 3542(b)(2)” and inserting “section 3552(b)”.

10 (F) IKE SKELTON NATIONAL DEFENSE AU-
 11 THORIZATION ACT FOR FISCAL YEAR 2011.—The
 12 Ike Skelton National Defense Authorization Act
 13 for Fiscal Year 2011 (Public Law 111–383) is
 14 amended—

15 (i) in section 806(e)(5) (10 U.S.C.
 16 2304 note), by striking “section 3542(b)”
 17 and inserting “section 3552(b)”;

18 (ii) in section 931(b)(3) (10 U.S.C.
 19 2223 note), by striking “section
 20 3542(b)(2)” and inserting “section
 21 3552(b)”;

22 (iii) in section 932(b)(2) (10 U.S.C.
 23 2224 note), by striking “section
 24 3542(b)(2)” and inserting “section
 25 3552(b)”.

1 (G) E-GOVERNMENT ACT OF 2002.—Sec-
 2 tion 301(c)(1)(A) of the E-Government Act of
 3 2002 (44 U.S.C. 3501 note) is amended by
 4 striking “section 3542(b)(2)” and inserting
 5 “section 3552(b)”.

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

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

13 (ii) in subsection (f)—

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

17 (II) in paragraph (5), by striking
 18 “section 3532(b)(2)” and inserting
 19 “section 3552(b)”.

20 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II
 21 of chapter 35 of title 44, United States Code, is amend-
 22 ed—

23 (1) in section 3551—

1 (A) in paragraph (4), by striking “diag-
2 nose and improve” and inserting “integrate, de-
3 liver, diagnose, and improve”;

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

6 (C) in paragraph (6), by striking the pe-
7 riod at the end and inserting a semi colon; and

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

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

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

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

21 (2) in section 3553—

22 (A) in subsection (a)—

23 (i) in paragraph (1), by inserting “, in
24 consultation with the Secretary and the

1 National Cyber Director,” before “over-
2 seeing”;

3 (ii) in paragraph (5), by striking
4 “and” at the end; and

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

7 “(8) promoting, in consultation with the Direc-
8 tor of the Cybersecurity and Infrastructure Security
9 Agency, the National Cyber Director, and the Direc-
10 tor of the National Institute of Standards and Tech-
11 nology—

12 “(A) the use of automation to improve
13 Federal cybersecurity and visibility with respect
14 to the implementation of Federal cybersecurity;
15 and

16 “(B) the use of presumption of com-
17 promise and least privilege principles to improve
18 resiliency and timely response actions to inci-
19 dents on Federal systems.”;

20 (B) in subsection (b)—

21 (i) in the matter preceding paragraph
22 (1), by inserting “and the National Cyber
23 Director” after “Director”; and

24 (ii) in paragraph (2)(A), by inserting
25 “and reporting requirements under sub-

1 chapter IV of this chapter” after “section
2 3556”; and

3 (C) in subsection (c)—

4 (i) in the matter preceding paragraph
5 (1)—

6 (I) by striking “each year” and
7 inserting “each year during which
8 agencies are required to submit re-
9 ports under section 3554(c)”; and

10 (II) by striking “preceding year”
11 and inserting “preceding 2 years”;

12 (ii) by striking paragraph (1);

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

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

18 (v) by inserting after paragraph (3),
19 as so redesignated the following:

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

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

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

4 (E) by inserting after subsection (h) the
5 following:

6 “(i) FEDERAL RISK ASSESSMENTS.—On an ongoing
7 and continuous basis, the Director of the Cybersecurity
8 and Infrastructure Security Agency shall perform assess-
9 ments of Federal risk posture using any available informa-
10 tion on the cybersecurity posture of agencies, and brief
11 the Director and National Cyber Director on the findings
12 of those assessments including—

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

15 “(2) any vulnerability information relating to
16 the systems of an agency that is known by the agen-
17 cy;

18 “(3) analysis of incident information under sec-
19 tion 3597;

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

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

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

1 “(7) evaluation of Federal and non-Federal
2 cyber threat intelligence;

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

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

7 “(10) any other information the Director of the
8 Cybersecurity and Infrastructure Security Agency
9 determines relevant.”;

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

11 (i) by striking “regarding the spe-
12 cific” and inserting “that includes a sum-
13 mary of—

14 “(1) the specific”;

15 (ii) in paragraph (1), as so des-
16 ignated, by striking the period at the end
17 and inserting “; and” and

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

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

22 (G) by adding at the end the following:

23 “(n) BINDING OPERATIONAL DIRECTIVES.—If the
24 Director of the Cybersecurity and Infrastructure Security
25 Agency issues a binding operational directive or an emer-

1 gency directive under this section, not later than 4 days
 2 after the date on which the binding operational directive
 3 requires an agency to take an action, the Director of the
 4 Cybersecurity and Infrastructure Security Agency shall
 5 provide to the Director, National Cyber Director, the
 6 Committee on Homeland Security and Governmental Af-
 7 fairs of the Senate and the Committee on Oversight and
 8 Reform of the House of Representatives the status of the
 9 implementation of the binding operational directive at the
 10 agency.”;

11 (3) in section 3554—

12 (A) in subsection (a)—

13 (i) in paragraph (1)—

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

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

20 “(A) on an ongoing and continuous basis,
 21 performing agency system risk assessments
 22 that—

23 “(i) identify and document the high
 24 value assets of the agency using guidance
 25 from the Director;

1 “(ii) evaluate the data assets inven-
2 toried under section 3511 for sensitivity to
3 compromises in confidentiality, integrity,
4 and availability;

5 “(iii) identify agency systems that
6 have access to or hold the data assets
7 inventoried under section 3511;

8 “(iv) evaluate the threats facing agen-
9 cy systems and data, including high value
10 assets, based on Federal and non-Federal
11 cyber threat intelligence products, where
12 available;

13 “(v) evaluate the vulnerability of
14 agency systems and data, including high
15 value assets, including by analyzing—

16 “(I) the results of penetration
17 testing performed by the Department
18 of Homeland Security under section
19 3553(b)(9);

20 “(II) the results of penetration
21 testing performed under section
22 3559A;

23 “(III) information provided to
24 the agency through the vulnerability

1 disclosure program of the agency
2 under section 3559B;

3 “(IV) incidents; and

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

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

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

20 (III) in subparagraph (B), as so
21 redesignated, in the matter preceding
22 clause (i), by striking “providing in-
23 formation” and inserting “using infor-
24 mation from the assessment con-

1 ducted under subparagraph (A), pro-
2 viding information”;

3 (IV) in subparagraph (C), as so
4 redesignated—

5 (aa) in clause (ii) by insert-
6 ing “binding” before “oper-
7 ational”; and

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

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

12 “(E) providing an update on the ongoing
13 and continuous assessment performed under
14 subparagraph (A)—

15 “(i) upon request, to the inspector
16 general of the agency or the Comptroller
17 General of the United States; and

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

21 “(I) the Director;

22 “(II) the Director of the Cyberse-
23 curity and Infrastructure Security
24 Agency; and

1 “(III) the National Cyber Direc-
2 tor;

3 “(F) in consultation with the Director of
4 the Cybersecurity and Infrastructure Security
5 Agency and not less frequently than once every
6 3 years, performing an evaluation of whether
7 additional cybersecurity procedures are appro-
8 priate for securing a system of, or under the
9 supervision of, the agency, which shall—

10 “(i) be completed considering the
11 agency system risk assessment performed
12 under subparagraph (A); and

13 “(ii) include a specific evaluation for
14 high value assets;

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

21 “(i) the Director of the Cybersecurity
22 and Infrastructure Security Agency;

23 “(ii) the Director; and

24 “(iii) the National Cyber Director;

25 and

“(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency;”;

(ii) in paragraph (2)—

(I) in subparagraph (A), by inserting “in accordance with the agency system risk assessment performed under paragraph (1)(A)” after “information systems”;

(II) in subparagraph (B)—

(aa) by striking “in accordance with standards” and inserting “in accordance with—

“(i) standards”; and

(bb) by adding at the end the following:

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

“(iii) the implementation plan described in paragraph (1)(G);”;

(III) in subparagraph (D), by inserting “, through the use of penetration testing, the vulnerability disclo-

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

4 (iii) in paragraph (3)—

5 (I) in subparagraph (A)—

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

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

10 (cc) by adding at the end
 11 the following:

12 “(v) ensure that—

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

20 “(II) senior agency information
 21 security officers of component agen-
 22 cies report to—

23 “(aa) the senior information
 24 security officer of the agency or
 25 an equivalent official; and

1 “(bb) the Chief Information
 2 Officer of the component agency
 3 or an equivalent official;”; and

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

8 (B) in subsection (b)—

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

11 “(1) pursuant to subsection (a)(1)(A), per-
 12 forming ongoing and continuous agency system risk
 13 assessments, which may include using guidelines and
 14 automated tools consistent with standards and
 15 guidelines promulgated under section 11331 of title
 16 40, as applicable;”;

17 (ii) in paragraph (2)—

18 (I) by striking subparagraph (B)
 19 and inserting the following:

20 “(B) comply with the risk-based cyber
 21 budget model developed pursuant to section
 22 3553(a)(7);”; and

23 (II) in subparagraph (D)—

1 (aa) by redesignating
 2 clauses (iii) and (iv) as clauses
 3 (iv) and (v), respectively;

4 (bb) by inserting after
 5 clause (ii) the following:

6 “(iii) binding operational directives
 7 and emergency directives promulgated by
 8 the Director of the Cybersecurity and In-
 9 frastructure Security Agency under section
 10 3553;”; and

11 (cc) in clause (iv), as so re-
 12 designated, by striking “as deter-
 13 mined by the agency; and” and
 14 inserting “as determined by the
 15 agency, considering—

16 “(I) the agency risk assessment
 17 performed under subsection (a)(1)(A);
 18 and

19 “(II) the determinations of ap-
 20 plying more stringent standards and
 21 additional cybersecurity procedures
 22 pursuant to section 11331(c)(1) of
 23 title 40; and”;

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

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

11 (v) by redesignating paragraphs (7)
 12 and (8) as paragraphs (8) and (9), respec-
 13 tively;

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

16 “(7) a process for providing the status of every
 17 remedial action and unremediated identified system
 18 vulnerability to the Director and the Director of the
 19 Cybersecurity and Infrastructure Security Agency,
 20 using automation and machine-readable data to the
 21 greatest extent practicable;” and

22 (vii) in paragraph (8)(C), as so redес-
 23 ignated—

24 (I) by striking clause (ii) and in-
 25 serting the following:

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

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

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

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

(IV) in clause (iv), as so redesignated—

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

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

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

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

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

3 “(1) BIENNIAL REPORT.—Not later than 2
4 years after the date of enactment of the Federal In-
5 formation Security Modernization Act of 2022 and
6 not less frequently than once every 2 years there-
7 after, using the continuous and ongoing agency sys-
8 tem risk assessment under subsection (a)(1)(A), the
9 head of each agency shall submit to the Director,
10 the Director of the Cybersecurity and Infrastructure
11 Security Agency, the majority and minority leaders
12 of the Senate, the Speaker and minority leader of
13 the House of Representatives, the Committee on
14 Homeland Security and Governmental Affairs of the
15 Senate, the Committee on Oversight and Reform of
16 the House of Representatives, the Committee on
17 Homeland Security of the House of Representatives,
18 the Committee on Commerce, Science, and Trans-
19 portation of the Senate, the Committee on Science,
20 Space, and Technology of the House of Representa-
21 tives, the appropriate authorization and appropria-
22 tions committees of Congress, the National Cyber
23 Director, and the Comptroller General of the United
24 States a report that—

1 “(A) summarizes the agency system risk
2 assessment performed under subsection
3 (a)(1)(A);

4 “(B) evaluates the adequacy and effective-
5 ness of information security policies, proce-
6 dures, and practices of the agency to address
7 the risks identified in the agency system risk
8 assessment performed under subsection
9 (a)(1)(A), including an analysis of the agency’s
10 cybersecurity and incident response capabilities
11 using the metrics established under section
12 224(c) of the Cybersecurity Act of 2015 (6
13 U.S.C. 1522(c));

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

21 “(D) summarizes the status of remedial
22 actions identified by inspector general of the
23 agency, the Comptroller General of the United
24 States, and any other source determined appro-
25 priate by the head of the agency.

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

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

6 “(B) may include a classified annex.

7 “(3) ACCESS TO INFORMATION.—The head of
8 an agency shall ensure that, to the greatest extent
9 practicable, information is included in the unclassi-
10 fied form of the report submitted by the agency
11 under paragraph (2)(A).

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

18 (iii) in paragraph (5), as so redesign-
19 nated, by striking the period at the end
20 and inserting “, including the reporting
21 procedures established under section
22 11315(d) of title 40 and subsection
23 (a)(3)(A)(v) of this section”; and

24 (D) in subsection (d)(1), in the matter pre-
25 ceding subparagraph (A), by inserting “and the

1 National Cyber Director” after “the Director”;
 2 and

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

4 “(f) REPORTING STRUCTURE EXEMPTION.—

5 “(1) IN GENERAL.—On an annual basis, the
 6 Director may exempt an agency from the reporting
 7 structure requirement under subsection
 8 (a)(3)(A)(v)(II).

9 “(2) REPORT.—On an annual basis, the Direc-
 10 tor shall submit a report to the Committee on
 11 Homeland Security and Governmental Affairs of the
 12 Senate and the Committee on Oversight and Reform
 13 of the House of Representatives that includes a list
 14 of each exemption granted under paragraph (1) and
 15 the associated rationale for each exemption.

16 “(3) COMPONENT OF OTHER REPORT.—The re-
 17 port required under paragraph (2) may be incor-
 18 porated into any other annual report required under
 19 this chapter.”;

20 (4) in section 3555—

21 (A) in the section heading, by striking
 22 “**ANNUAL INDEPENDENT**” and inserting
 23 “**INDEPENDENT**”;

24 (B) in subsection (a)—

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

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

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

12 “(3) An evaluation under this section may include
 13 recommendations for improving the cybersecurity posture
 14 of the agency.”;

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

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

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

22 “(f) PROTECTION OF INFORMATION.—(1) Agencies,
 23 evaluators, and other recipients of information that, if dis-
 24 closed, may cause grave harm to the efforts of Federal
 25 information security officers, shall take appropriate steps

1 to ensure the protection of that information, including
 2 safeguarding the information from public disclosure.

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

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

11 “(A) specific information system incidents; or

12 “(B) specific information system
 13 vulnerabilities.”;

14 (F) in subsection (g)(2)—

15 (i) by striking “this subsection shall”

16 and inserting “this subsection—

17 “(A) shall”;

18 (ii) in subparagraph (A), as so des-
 19 ignated, by striking the period at the end
 20 and inserting “; and”; and

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

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

1 (G) by striking subsection (j) and inserting
2 the following:

3 “(j) GUIDANCE.—

4 “(1) IN GENERAL.—The Director, in consulta-
5 tion with the Director of the Cybersecurity and In-
6 frastructure Security Agency, the Chief Information
7 Officers Council, the Council of the Inspectors Gen-
8 eral on Integrity and Efficiency, and other interested
9 parties as appropriate, shall ensure the development
10 of risk-based guidance for evaluating the effective-
11 ness of an information security program and prac-
12 tices

13 “(2) PRIORITIES.—The risk-based guidance de-
14 veloped under paragraph (1) shall include—

15 “(A) the identification of the most common
16 successful threat patterns experienced by each
17 agency;

18 “(B) the identification of security controls
19 that address the threat patterns described in
20 subparagraph (A);

21 “(C) any other security risks unique to the
22 networks of each agency; and

23 “(D) any other element the Director, in
24 consultation with the Director of the Cybersecu-
25 rity and Infrastructure Security Agency and the

Council of the Inspectors General on Integrity and Efficiency, determines appropriate.”; and (5) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting “within the Cybersecurity and Infrastructure Security Agency” after “incident center”; and

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

(d) CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3555 and inserting the following:

“3555. Independent evaluation”.

(2) OMB REPORTS.—Section 226(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1524(c)) is amended—

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

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

1 (i) by striking “annually thereafter”
 2 and inserting “thereafter during the years
 3 during which a report is required to be
 4 submitted under section 3553(c) of title
 5 44, United States Code”; and

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

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

13 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

17 “SUBCHAPTER IV—FEDERAL SYSTEM
 18 INCIDENT RESPONSE

19 **“§ 3591. Definitions**

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

23 “(b) ADDITIONAL DEFINITIONS.—As used in this
 24 subchapter:

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

3 “(A) the majority and minority leaders of
4 the Senate;

5 “(B) the Speaker and minority leader of
6 the House of Representatives;

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

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

11 “(E) the Committee on Homeland Security
12 of the House of Representatives;

13 “(F) the appropriate authorization and ap-
14 propriations committees of Congress;

15 “(G) the Director;

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

18 “(I) the National Cyber Director;

19 “(J) the Comptroller General of the United
20 States; and

21 “(K) the inspector general of any impacted
22 agency.

23 “(2) AWARDEE.—The term ‘awardee’—

24 “(A) means a person, business, or other
25 entity that receives a grant from, or is a party

1 to a cooperative agreement or an other trans-
 2 action agreement with, an agency; and

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

6 “(3) BREACH.—The term ‘breach’—

7 “(A) means the loss, control, compromise,
 8 unauthorized disclosure, or unauthorized acqui-
 9 sition of personally identifiable information or
 10 any similar occurrence; and

11 “(B) includes any additional meaning
 12 given the term in policies, principles, standards,
 13 or guidelines issued by the Director under sec-
 14 tion 3553(a).

15 “(4) CONTRACTOR.—The term ‘contractor’
 16 means a prime contractor of an agency or a subcon-
 17 tractor of a prime contractor of an agency.

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

23 “(6) FEDERAL INFORMATION SYSTEM.—The
 24 term ‘Federal information system’ means an infor-
 25 mation system used or operated by an agency, a con-

1 tractor, an awardee, or another organization on be-
 2 half of an agency.

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

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

12 “(9) VULNERABILITY DISCLOSURE.—The term
 13 ‘vulnerability disclosure’ means a vulnerability iden-
 14 tified under section 3559B.

15 **“§ 3592. Notification of breach**

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

22 “(1) determine whether notice to any individual
 23 potentially affected by the breach is appropriate
 24 based on an assessment of the risk of harm to the
 25 individual that considers—

1 “(A) the nature and sensitivity of the per-
2 sonally identifiable information affected by the
3 breach;

4 “(B) the likelihood of access to and use of
5 the personally identifiable information affected
6 by the breach;

7 “(C) the type of breach; and

8 “(D) any other factors determined by the
9 Director; and

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

13 “(A) to the last known mailing address of
14 the individual; or

15 “(B) through an appropriate alternative
16 method of notification that the head of the
17 agency or a designated senior-level individual of
18 the agency selects based on factors determined
19 by the Director.

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

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

1 “(2) if possible, a description of the types of
2 personally identifiable information affected by the
3 breach;

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

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

8 “(B) may include a telephone number,
9 mailing address, or a website;

10 “(4) information on any remedy being offered
11 by the agency;

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

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

21 “(c) DELAY OF NOTIFICATION.—

22 “(1) IN GENERAL.—The Attorney General, the
23 Director of National Intelligence, or the Secretary of
24 Homeland Security may delay a notification required

1 under subsection (a) or (d) if the notification
2 would—

3 “(A) impede a criminal investigation or a
4 national security activity;

5 “(B) reveal sensitive sources and methods;

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

7 “(D) hamper security remediation actions.

8 “(2) DOCUMENTATION.—

9 “(A) IN GENERAL.—Any delay under para-
10 graph (1) shall be reported in writing to the Di-
11 rector, the Attorney General, the Director of
12 National Intelligence, the Secretary of Home-
13 land Security, the National Cyber Director, the
14 Director of the Cybersecurity and Infrastruc-
15 ture Security Agency, and the head of the agen-
16 cy and the inspector general of the agency that
17 experienced the breach.

18 “(B) CONTENTS.—A report required under
19 subparagraph (A) shall include a written state-
20 ment from the entity that delayed the notifica-
21 tion explaining the need for the delay.

22 “(C) FORM.—The report required under
23 subparagraph (A) shall be unclassified but may
24 include a classified annex.

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

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

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

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

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

1 **“§ 3593. Congressional and Executive Branch reports**

2 “(a) INITIAL REPORT.—

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

16 “(A) the information known at the time of
17 the report;

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

20 “(C) the classification level of the informa-
21 tion contained in the report.

22 “(2) CONTENTS.—A report required under
23 paragraph (1) shall include, in a manner that ex-
24 cludes or otherwise reasonably protects personally
25 identifiable information and to the extent permitted

1 by applicable law, including privacy and statistical
2 laws—

3 “(A) a summary of the information avail-
4 able about the major incident, including how
5 the major incident occurred, information indi-
6 cating that the major incident may be a breach,
7 and information relating to the major incident
8 as a breach, based on information available to
9 agency officials as of the date on which the
10 agency submits the report;

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

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

22 “(D) if applicable, whether any ransom has
23 been demanded or paid, or plans to be paid, by
24 any entity operating a Federal information sys-
25 tem or with access to a Federal information

1 system, unless disclosure of such information
2 may disrupt an active Federal law enforcement
3 or national security operation.

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

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

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

21 “(3) the status of compliance of the affected in-
22 formation system with applicable security require-
23 ments that are directly related to the cause of the
24 incident, 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;

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 described in section
21 3592(c), if applicable; and

22 “(8) if applicable, a description of any cir-
23 cumstances or data leading the head of the agency
24 to determine, pursuant to section 3592(a)(1), not to
25 notify individuals potentially impacted by a breach.

1 “(c) UPDATE REPORT.—If the agency determines
 2 that there is any significant change in the understanding
 3 of the agency of the scope, scale, or consequence of a
 4 major incident for which an agency submitted a written
 5 report under subsection (a), the agency shall provide an
 6 updated report to the appropriate reporting entities that
 7 includes information relating to the change in under-
 8 standing.

9 “(d) BIENNIAL REPORT.—Each agency shall submit
 10 as part of the biannual report required under section
 11 3554(c)(1) of this title a description of each major inci-
 12 dent that occurred during the 2-year period preceding the
 13 date on which the biannual report is submitted.

14 “(e) DELAY AND LACK OF NOTIFICATION REPORT.—

15 “(1) IN GENERAL.—The Director shall submit
 16 to the appropriate reporting entities an annual re-
 17 port on all notification delays granted pursuant to
 18 section 3592(c).

19 “(2) LACK OF BREACH NOTIFICATION.—The
 20 Director shall submit to the appropriate reporting
 21 entities an annual report on each breach with re-
 22 spect to which the head of an agency determined,
 23 pursuant to section 3592(a)(1), not to notify individ-
 24 uals potentially impacted by the breach.

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

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

8 “(g) THREAT BRIEFING.—

9 “(1) IN GENERAL.—Not later than 7 days after
 10 the date on which an agency has a reasonable basis
 11 to conclude that a major incident occurred, the head
 12 of the agency, jointly with the Director, the National
 13 Cyber Director and any other Federal entity deter-
 14 mined appropriate by the National Cyber Director,
 15 shall provide a briefing to the congressional commit-
 16 tees described in subsection (a)(1) on the threat
 17 causing the major incident.

18 “(2) COMPONENTS.—The briefing required
 19 under paragraph (1)—

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

22 “(B) may include a classified component.

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

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

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

6 **“§ 3594. Government information sharing and inci-**
 7 **dent response**

8 “(a) IN GENERAL.—

9 “(1) INCIDENT REPORTING.—Subject to the
 10 limitations described in subsection (b), the head of
 11 each agency shall provide any information relating
 12 to any incident affecting the agency, whether the in-
 13 formation is obtained by the Federal Government di-
 14 rectly or indirectly, to the Cybersecurity and Infra-
 15 structure Security Agency.

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

19 “(A) include detailed information about
 20 the safeguards that were in place when the inci-
 21 dent occurred;

22 “(B) whether the agency implemented the
 23 safeguards described in subparagraph (A) cor-
 24 rectly;

1 “(C) in order to protect against a similar
2 incident, identify—

3 “(i) how the safeguards described in
4 subparagraph (A) should be implemented
5 differently; and

6 “(ii) additional necessary safeguards;
7 and

8 “(D) include information to aid in incident
9 response, such as—

10 “(i) a description of the affected sys-
11 tems or networks;

12 “(ii) the estimated dates of when the
13 incident occurred; and

14 “(iii) information that could reason-
15 ably help identify the party that conducted
16 the incident or the cause of the incident,
17 subject to appropriate privacy protections.

18 “(3) INFORMATION SHARING.—The Director of
19 the Cybersecurity and Infrastructure Security Agen-
20 cy shall—

21 “(A) make incident information provided
22 under paragraph (1) available to the Director
23 and the National Cyber Director;

1 “(B) to the greatest extent practicable,
2 share information relating to an incident with
3 the head of any agency that may be—

4 “(i) impacted by the incident;

5 “(ii) similarly susceptible to the inci-
6 dent; or

7 “(iii) similarly targeted by the inci-
8 dent; and

9 “(C) coordinate any necessary information
10 sharing efforts relating to a major incident with
11 the private sector.

12 “(4) NATIONAL SECURITY SYSTEMS.—Each
13 agency operating or exercising control of a national
14 security system shall share information about inci-
15 dents that occur on national security systems with
16 the Director of the Cybersecurity and Infrastructure
17 Security Agency to the extent consistent with stand-
18 ards and guidelines for national security systems
19 issued in accordance with law and as directed by the
20 President.

21 “(b) COMPLIANCE.—In providing information and se-
22 lecting a method to provide information under subsection
23 (a), the head of each agency shall take into account the
24 level of classification of the information and any informa-
25 tion sharing limitations and protections, such as limita-

1 tions and protections relating to law enforcement, national
 2 security, privacy, statistical confidentiality, or other fac-
 3 tors determined by the Director in order to implement
 4 subsection (a)(1) in a manner that enables automated and
 5 consistent reporting to the greatest extent practicable.

6 “(c) INCIDENT RESPONSE.—Each agency that has a
 7 reasonable basis to conclude that a major incident oc-
 8 curred involving Federal information in electronic medium
 9 or form that does not exclusively involve a national secu-
 10 rity system, regardless of delays from notification granted
 11 for a major incident that is also a breach, shall coordinate
 12 with the Cybersecurity and Infrastructure Security Agen-
 13 cy to facilitate asset response activities and provide rec-
 14 ommendations for mitigating future incidents.

15 **“§ 3595. Responsibilities of contractors and awardees**

16 “(a) REPORTING.—

17 “(1) IN GENERAL.—Unless otherwise specified
 18 in a contract, grant, cooperative agreement, or an
 19 other transaction agreement, any contractor or
 20 awardee of an agency shall report to the agency
 21 within the same amount of time such agency is re-
 22 quired to report an incident to the Cybersecurity
 23 and Infrastructure Security Agency, if the con-
 24 tractor or awardee has a reasonable basis to suspect
 25 or conclude that—

1 “(A) an incident or breach has occurred
2 with respect to Federal information collected,
3 used, or maintained by the contractor or award-
4 ee in connection with the contract, grant, coop-
5 erative agreement, or other transaction agree-
6 ment of the contractor or awardee;

7 “(B) an incident or breach has occurred
8 with respect to a Federal information system
9 used or operated by the contractor or awardee
10 in connection with the contract, grant, coopera-
11 tive agreement, or other transaction agreement
12 of the contractor or awardee; or

13 “(C) the contractor or awardee has re-
14 ceived information from the agency that the
15 contractor or awardee is not authorized to re-
16 ceive in connection with the contract, grant, co-
17 operative agreement, or other transaction agree-
18 ment of the contractor or awardee.

19 “(2) PROCEDURES.—

20 “(A) MAJOR INCIDENT.—Following a re-
21 port of a breach or major incident by a con-
22 tractor or awardee under paragraph (1), the
23 agency, in consultation with the contractor or
24 awardee, shall carry out the requirements under

1 sections 3592, 3593, and 3594 with respect to
 2 the major incident.

3 “(B) INCIDENT.—Following a report of an
 4 incident by a contractor or awardee under para-
 5 graph (1), an agency, in consultation with the
 6 contractor or awardee, shall carry out the re-
 7 quirements under section 3594 with respect to
 8 the incident.

9 “(b) EFFECTIVE DATE.—This section shall apply—
 10 “(1) on and after the date that is 1 year after
 11 the date of enactment of the Federal Information
 12 Security Modernization Act of 2022; and

13 “(2) with respect to any contract entered into
 14 on or after the date described in paragraph (1).

15 **“§ 3596. Training**

16 “(a) COVERED INDIVIDUAL DEFINED.—In this sec-
 17 tion, the term ‘covered individual’ means an individual
 18 who obtains access to Federal information or Federal in-
 19 formation systems because of the status of the individual
 20 as an employee, contractor, awardee, volunteer, or intern
 21 of an agency.

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

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

3 “(2) the obligation of a covered individual to re-
 4 port to the agency a confirmed major incident and
 5 any suspected incident involving information in any
 6 medium or form, including paper, oral, and elec-
 7 tronic.

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

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

13 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

14 “(1) 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 incidents at agen-
 20 cies, including major incidents, including—

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

22 “(i) attacker tactics, techniques, and
 23 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 incidents at
5 agencies;

6 “(C) common root causes of incidents
7 across multiple Federal agencies;

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

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

14 “(F) trends across multiple Federal agen-
15 cies to address intrusion detection and incident
16 response capabilities using the metrics estab-
17 lished under section 224(c) of the Cybersecurity
18 Act of 2015 (6 U.S.C. 1522(c)).

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

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

24 “(A) IN GENERAL.—The Director shall
25 share on an ongoing basis the analyses required

1 under this subsection with agencies and the Na-
2 tional Cyber Director to—

3 “(i) improve the understanding of cy-
4 bersecurity risk of agencies; and

5 “(ii) support the cybersecurity im-
6 provement efforts of agencies.

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

10 “(i) in human-readable written prod-
11 ucts; and

12 “(ii) to the greatest extent practicable,
13 in machine-readable formats in order to
14 enable automated intake and use by agen-
15 cies.

16 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—
17 Not later than 2 years after the date of enactment of this
18 section, and not less frequently than annually thereafter,
19 the Director of the Cybersecurity and Infrastructure Secu-
20 rity Agency, in consultation with the Director, the Na-
21 tional Cyber Director and the heads of other Federal agen-
22 cies, as appropriate, shall submit to the appropriate re-
23 porting entities a report that includes—

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

4 “(2) the quantitative and qualitative analyses of
5 incidents developed under subsection (a)(1) on an
6 agency-by-agency basis and comprehensively across
7 the Federal Government, including—

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

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

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

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

15 “(B) the total number of incidents of the
16 agency; and

17 “(C) an analysis of the agency’s perform-
18 ance against the metrics established under sec-
19 tion 224(c) of the Cybersecurity Act of 2015 (6
20 U.S.C. 1522(c)).

21 “(c) PUBLICATION.—

22 “(1) IN GENERAL.—A version of each report
23 submitted under subsection (b) shall be made pub-
24 licly available on the website of the Cybersecurity

1 and Infrastructure Security Agency during the year
2 in which the report is submitted.

3 “(2) EXEMPTION.—The Director of the Cyber-
4 security and Infrastructure Security Agency may ex-
5 empt all or a portion of a report described in para-
6 graph (1) from public publication if the Director of
7 the Cybersecurity and Infrastructure Security Agen-
8 cy determines the exemption is in the interest of na-
9 tional security.

10 “(3) LIMITATION ON EXEMPTION.—An exemp-
11 tion granted under paragraph (2) shall not apply to
12 any version of a report submitted to the appropriate
13 reporting entities under subsection (b).

14 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

19 “(2) NONCOMPLIANCE REPORTS.—

20 “(A) IN GENERAL.—Subject to subpara-
21 graph (B), during any year during which the
22 head of an agency does not provide data for an
23 incident to the Cybersecurity and Infrastructure
24 Security Agency in accordance with section
25 3594(a), the head of the agency, in coordina-

tion with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes the information described in subsection (b) with respect to the agency.

“(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

“(3) NATIONAL SECURITY SYSTEM REPORTS.—

“(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the national security system to the extent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

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

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

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

6 “(iv) the Select Committee on Intel-
7 ligence of the Senate;

8 “(v) the Committee on Armed Serv-
9 ices of the Senate;

10 “(vi) the Committee on Appropria-
11 tions of the Senate;

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

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

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

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

21 “(xi) the Committee on Appropria-
22 tions of the House of Representatives.

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

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

9 **“§ 3598. Major incident definition**

10 “(a) IN GENERAL.—Not later than 180 days after
 11 the date of enactment of the Federal Information Security
 12 Modernization Act of 2022, the Director, in coordination
 13 with the Director of the Cybersecurity and Infrastructure
 14 Security Agency and the National Cyber Director, shall
 15 develop and promulgate guidance on the definition of the
 16 term ‘major incident’ for the purposes of subchapter II
 17 and this subchapter.

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

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

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

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

6 “(ii) the civil liberties or public health
7 and safety of the people of the United
8 States;

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

14 “(C) any incident that the head of an
15 agency, in consultation with a senior privacy of-
16 ficer of the agency, determines is likely to have
17 a significant privacy impact on 1 or more indi-
18 vidual;

19 “(D) any incident that the head of the
20 agency, in consultation with a senior privacy of-
21 ficial of the agency, determines is likely to have
22 a substantial privacy impact on a significant
23 number of individuals;

24 “(E) any incident the head of the agency
25 determines substantially disrupts the operations

1 of a high value asset owned or operated by the
2 agency;

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

9 “(G) any other type of incident determined
10 appropriate by the Director;

11 “(2) stipulate that the National Cyber Director,
12 in consultation with the Director, shall declare a
13 major incident at each agency impacted by an inci-
14 dent if it is determined that an incident—

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

16 and

17 “(B) is enabled by—

18 “(i) a common technical root cause,
19 such as a supply chain compromise, a com-
20 mon software or hardware vulnerability; or

21 “(ii) the related activities of a com-
22 mon threat actor; and

23 “(3) stipulate that, in determining whether an
24 incident constitutes a major incident because that
25 incident is any incident described in paragraph (1),

1 the head of the agency shall consult with the Na-
2 tional Cyber Director and may consult with the Di-
3 rector of the Cybersecurity and Infrastructure Secu-
4 rity Agency.

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

8 “(1) may determine a threshold for a minimum
9 number of individuals that constitutes a significant
10 amount; and

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

13 “(d) EVALUATION AND UPDATES.—Not later than 2
14 years after the date of enactment of the Federal Informa-
15 tion Security Modernization Act of 2022, and not less fre-
16 quently than every 2 years thereafter, the Director shall
17 provide a briefing to the Committee on Homeland Security
18 and Governmental Affairs of the Senate and the Com-
19 mittee on Oversight and Reform of the House of Rep-
20 resentatives, which shall include—

21 “(1) an evaluation of any necessary updates to
22 the guidance issued under subsection (a);

23 “(2) an evaluation of any necessary updates to
24 the definition of the term ‘major incident’ included
25 in the guidance issued under subsection (a); and

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

3 (2) CLERICAL AMENDMENT.—The table of sec-
4 tions for chapter 35 of title 44, United States Code,
5 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”.

6 **SEC. 104. AMENDMENTS TO SUBTITLE III OF TITLE 40.**

7 (a) MODERNIZING GOVERNMENT TECHNOLOGY.—
8 Subtitle G of title X of Division A of the National Defense
9 Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301
10 note) is amended in section 1078—

11 (1) by striking subsection (a) and inserting the
12 following:

13 “(a) DEFINITIONS.—In this section:

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

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

20 (2) in subsection (b), by adding at the end the
21 following:

1 “(8) PROPOSAL EVALUATION.—The Director
2 shall—

3 “(A) give consideration for the use of
4 amounts in the Fund to improve the security of
5 high value assets; and

6 “(B) require that any proposal for the use
7 of amounts in the Fund includes a cybersecu-
8 rity plan, including a supply chain risk manage-
9 ment plan, to be reviewed by the member of the
10 Technology Modernization Board described in
11 subsection (c)(5)(C).”; and

12 (3) in subsection (c)—

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

16 (B) in paragraph (5)—

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

19 (ii) in subparagraph (B), by striking
20 the period at the end and inserting “and”;
21 and

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

24 “(C) a senior official from the Cybersecu-
25 rity and Infrastructure Security Agency of the

1 Department of Homeland Security, appointed
 2 by the Director.”; and

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

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

8 (1) in section 11302—

9 (A) in subsection (b), by striking “use, se-
 10 curity, and disposal of” and inserting “use, and
 11 disposal of, and, in consultation with the Direc-
 12 tor of the Cybersecurity and Infrastructure Se-
 13 curity Agency and the National Cyber Director,
 14 promote and improve the security of,”;

15 (B) in subsection (c)—

16 (i) in paragraph (3)—

17 (I) in subparagraph (A)—

18 (aa) by striking “including
 19 data” and inserting “which
 20 shall—

21 “(i) include data”; and

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

24 “(ii) specifically denote cybersecurity
 25 funding under the risk-based cyber budget

1 model developed pursuant to section
2 3553(a)(7) of title 44.”; and

3 (II) in subparagraph (B), by add-
4 ing at the end the following:

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

11 (C) in subsection (f)—

12 (i) by striking “heads of executive
13 agencies to develop” and inserting “heads
14 of executive agencies to—

15 “(1) develop”;

16 (ii) in paragraph (1), as so des-
17 ignated, by striking the period at the end
18 and inserting “; and”; and

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

21 “(2) consult with the Director of the Cybersecu-
22 rity and Infrastructure Security Agency for the de-
23 velopment and use of supply chain security best
24 practices.”; and

1 (D) in subsection (h), by inserting “, in-
 2 cluding cybersecurity performances,” after “the
 3 performances”; and

4 (2) in section 11303(b)—

5 (A) in paragraph (2)(B)—

6 (i) in clause (i), by striking “or” at
 7 the end;

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

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

12 “(iii) whether the function should be
 13 performed by a shared service offered by
 14 another executive agency;”; and

15 (B) in paragraph (5)(B)(i), by inserting “,
 16 while taking into account the risk-based cyber
 17 budget model developed pursuant to section
 18 3553(a)(7) of title 44” after “title 31”.

19 (c) SUBCHAPTER II.—Subchapter II of chapter 113
 20 of subtitle III of title 40, United States Code, is amend-
 21 ed—

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

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

4 (3) in section 11315, by adding at the end the
5 following:

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

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

13 “(2) the head of the component agency.

14 “(e) REPORTING STRUCTURE EXEMPTION.—

15 “(1) IN GENERAL.—On annual basis, the Direc-
16 tor may exempt any agency from the reporting
17 structure requirements under subsection (d).

18 “(2) REPORT.—On an annual basis, the Direc-
19 tor shall submit to the Committee on Homeland Se-
20 curity and Governmental Affairs of the Senate and
21 the Committee on Oversight and Reform of the
22 House of Representatives a report that includes a
23 list of each exemption granted under paragraph (1)
24 and the associated rationale for each exemption.

1 “(3) COMPONENT OF OTHER REPORT.—The re-
 2 port required under paragraph (2) may be incor-
 3 porated into any other annual report required under
 4 chapter 35 of title 44, United States Code.”;

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

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

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

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

14 (2) in subsection (b)(1)(A), by striking “the
 15 Secretary of Homeland Security” and inserting “the
 16 Director of the Cybersecurity and Infrastructure Se-
 17 curity Agency”;

18 (3) by striking subsection (c) and inserting the
 19 following:

20 “(c) APPLICATION OF MORE STRINGENT STAND-
 21 ARDS.—

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

24 “(A) evaluate, in consultation with the sen-
 25 ior agency information security officers, the

1 need to employ standards for cost-effective,
2 risk-based information security for all systems,
3 operations, and assets within or under the su-
4 pervision of the agency that are more stringent
5 than the standards promulgated by the Director
6 under this section, if such standards contain, at
7 a minimum, the provisions of those applicable
8 standards made compulsory and binding by the
9 Director; and

10 “(B) to the greatest extent practicable and
11 if the head of the agency determines that the
12 standards described in subparagraph (A) are
13 necessary, employ those standards.

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

19 “(A) the status of cybersecurity remedial
20 actions of the agency;

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

23 “(C) incident information of the agency;

24 “(D) information from—

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

3 “(ii) information from the vulner-
4 ability disclosure program established
5 under section 3559B of title 44;

6 “(E) agency threat hunting results under
7 section 112 of the Federal Information Security
8 Modernization Act of 2022;

9 “(F) Federal and non-Federal cyber threat
10 intelligence;

11 “(G) data on compliance with standards
12 issued under this section;

13 “(H) agency system risk assessments per-
14 formed under section 3554(a)(1)(A) of title 44;
15 and

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

18 (4) in subsection (d)(2)—

19 (A) in the paragraph heading, by striking
20 “NOTICE AND COMMENT” and inserting “CON-
21 SULTATION, NOTICE, AND COMMENT”;

22 (B) by inserting “promulgate,” before
23 “significantly modify”; and

24 (C) by striking “shall be made after the
25 public is given an opportunity to comment on

1 the Director’s proposed decision.” and inserting
 2 “shall be made—

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

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

14 “(C) considering the Federal risk assess-
 15 ments performed under section 3553(i) of title
 16 44; and

17 “(D) considering the extent to which the
 18 proposed standard reduces risk relative to the
 19 cost of implementation of the standard.”; and
 20 (5) by adding at the end the following:

21 “(e) REVIEW OF OFFICE OF MANAGEMENT AND
 22 BUDGET GUIDANCE AND POLICY.—

23 “(1) CONDUCT OF REVIEW.—

24 “(A) IN GENERAL.—Not less frequently
 25 than once every 3 years, the Director of the Of-

1 fice of Management and Budget, in consultation
2 with the Chief Information Officers Council, the
3 Director of the Cybersecurity and Infrastruc-
4 ture Security Agency, the National Cyber Di-
5 rector, the Comptroller General of the United
6 States, and the Council of the Inspectors Gen-
7 eral on Integrity and Efficiency, shall review
8 the efficacy of the guidance and policy promul-
9 gated by the Director in reducing cybersecurity
10 risks, including an assessment of the require-
11 ments for agencies to report information to the
12 Director, and determine whether any changes to
13 that guidance or policy is appropriate.

14 “(B) FEDERAL RISK ASSESSMENTS.—In
15 conducting the review described in subpara-
16 graph (A), the Director shall consider the Fed-
17 eral risk assessments performed under section
18 3553(i) of title 44.

19 “(C) REQUIREMENTS BURDEN REDUCTION
20 AND CLARITY.—In conducting the review de-
21 scribed in subparagraph (A), the Director shall
22 consider—

23 “(i) the cumulative reporting and
24 compliance burden to agencies; and

1 “(ii) the clarity of the requirements
2 and deadlines contained in guidance and
3 policy documents.

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

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

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

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

22 “(C) a summary of the guidance or policy
23 to which changes were determined appropriate
24 during the review and what the changes are an-
25 ticipated to include.

1 “(4) CONGRESSIONAL BRIEFING.—Not later
 2 than 60 days after the date on which a review is
 3 completed under paragraph (1), the Director shall
 4 provide to the Committee on Homeland Security and
 5 Governmental Affairs of the Senate and the Com-
 6 mittee on Oversight and Reform of the House of
 7 Representatives a briefing on the review.

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

20 **SEC. 105. ACTIONS TO ENHANCE FEDERAL INCIDENT**
 21 **TRANSPARENCY.**

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

24 (1) IN GENERAL.—Not later than 180 days
 25 after the date of enactment of this Act, the Director

1 of the Cybersecurity and Infrastructure Security
2 Agency shall—

3 (A) develop a plan for the development of
4 the analysis required under section 3597(a) of
5 title 44, United States Code, as added by this
6 title, and the report required under subsection
7 (b) of that section that includes—

8 (i) a description of any challenges the
9 Director of the Cybersecurity and Infra-
10 structure Security Agency anticipates en-
11 countering; and

12 (ii) the use of automation and ma-
13 chine-readable formats for collecting, com-
14 piling, monitoring, and analyzing data; and

15 (B) provide to the appropriate congres-
16 sional committees a briefing on the plan devel-
17 oped under subparagraph (A).

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

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

1 (B) the development of the report required
 2 under section 3597(b) of title 44, United States
 3 Code, as added by this title.

4 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
 5 OFFICE OF MANAGEMENT AND BUDGET.—

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

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

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

13 (2) INCIDENT DATA SHARING.—

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

20 (B) REQUIREMENTS.—The guidance devel-
 21 oped under subparagraph (A) shall—

22 (i) prioritize the availability of data
 23 necessary to understand and analyze—

24 (I) the causes of incidents;

1 (II) the scope and scale of inci-
2 dents within the environments and
3 systems of an agency;

4 (III) a root cause analysis of in-
5 cidents that—

6 (aa) are common across the
7 Federal Government; or

8 (bb) have a Government-
9 wide impact;

10 (IV) agency response, recovery,
11 and remediation actions and the effec-
12 tiveness of those actions; and

13 (V) the impact of incidents;

14 (ii) enable the efficient development
15 of—

16 (I) lessons learned and rec-
17 ommendations in responding to, recov-
18 ering from, remediating, and miti-
19 gating future incidents; and

20 (II) the report on Federal inci-
21 dents required under section 3597(b)
22 of title 44, United States Code, as
23 added by this title;

24 (iii) include requirements for the time-
25 liness of data production; and

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

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

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

21 (5) CONTRACTOR AND AWARDEE GUIDANCE.—

22 (A) IN GENERAL.—Not later than 1 year
23 after the date of enactment of this Act, the Di-
24 rector, in coordination with the Secretary of
25 Homeland Security, the Secretary of Defense,

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

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

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

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

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

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

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

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

12 **SEC. 106. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**
13 **UPDATES.**

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

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

22 (2) implementing additional cybersecurity pro-
23 cedures, which shall include resources for shared
24 services;

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

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

10 (B) templates for providing the status of
 11 the remedial action; and

12 (4) a requirement to coordinate with inspectors
 13 general of agencies to ensure consistent under-
 14 standing and application of agency policies for the
 15 purpose of evaluations by inspectors general.

16 **SEC. 107. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**
 17 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

18 (a) DEFINITIONS.—In this section:

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

23 (2) SENSITIVE INFORMATION.—The term “sen-
 24 sitive information” has the meaning given the term

1 by the Director in guidance issued under subsection
 2 (b).

3 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-
 4 TITIES.—Not later than 180 days after the date of enact-
 5 ment of this Act, the Director shall issue guidance requir-
 6 ing the head of each agency to notify a reporting entity
 7 of an incident that is likely to substantially affect—

8 (1) the confidentiality or integrity of sensitive
 9 information submitted by the reporting entity to the
 10 agency pursuant to a statutory or regulatory re-
 11 quirement; or

12 (2) the agency information system or systems
 13 used in the transmission or storage of the sensitive
 14 information described in paragraph (1).

15 **SEC. 108. MOBILE SECURITY STANDARDS.**

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

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

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

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

24 (1) a requirement, pursuant to section
 25 3506(b)(4) of title 44, United States Code, for every

1 agency to maintain a continuous inventory of
2 every—

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

5 (B) vulnerability identified by the agency
6 associated with a mobile device; and

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

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

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

1 **SEC. 109. DATA AND LOGGING RETENTION FOR INCIDENT**
2 **RESPONSE.**

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

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

- 13 (1) the types of logs to be maintained;
- 14 (2) the duration that logs and other relevant
15 data should be retained;
- 16 (3) the time periods for agency implementation
17 of recommended logging and security requirements;
- 18 (4) how to ensure the confidentiality, integrity,
19 and availability of logs;
- 20 (5) requirements to ensure that, upon request,
21 in a manner that excludes or otherwise reasonably
22 protects personally identifiable information, and to
23 the extent permitted by applicable law (including
24 privacy and statistical laws), agencies provide logs
25 to—

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

4 (B) the Director of the Federal Bureau of
5 Investigation, or the appropriate Federal law
6 enforcement agency, to investigate potential
7 criminal activity; and

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

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

23 (d) SUNSET.—This section shall cease to have force
24 or effect on the date that is 10 years after the date of
25 the enactment of this Act.

1 **SEC. 110. CISA AGENCY ADVISORS.**

2 (a) IN GENERAL.—Not later than 120 days after the
3 date of enactment of this Act, the Director of the Cyberse-
4 curity and Infrastructure Security Agency shall assign not
5 less than 1 cybersecurity professional employed by the Cy-
6 bersecurity and Infrastructure Security Agency to be the
7 Cybersecurity and Infrastructure Security Agency advisor
8 to the senior agency information security officer of each
9 agency.

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

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

14 (2) performing risk assessments of agency sys-
15 tems; and

16 (3) other Federal cybersecurity initiatives.

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

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

21 (2) serving as an incident response point of
22 contact between the assigned agency and the Cyber-
23 security and Infrastructure Security Agency; and

24 (3) familiarizing themselves with agency sys-
25 tems, processes, and procedures to better facilitate
26 support to the agency in responding to incidents.

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

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

6 **SEC. 111. FEDERAL PENETRATION TESTING POLICY.**

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

10 **“§ 3559A. Federal penetration testing**

11 “(a) DEFINITIONS.—In this section:

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

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

19 “(b) GUIDANCE.—

20 “(1) IN GENERAL.—The Director, in consulta-
21 tion with the Secretary, acting through the Director
22 of the Cybersecurity and Infrastructure Security
23 Agency, shall issue guidance to agencies that—

24 “(A) requires agencies to use, when and
25 where appropriate, penetration testing on agen-

1 cy systems by both Federal and non-Federal en-
2 tities; and

3 “(B) requires agencies to develop an agen-
4 cy operational plan and rules of engagement
5 that meet the requirements under subsection
6 (c).

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

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

11 “(i) a shared service of the agency or
12 another agency; or

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

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

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

24 “(1) require the agency to—

1 “(A) perform penetration testing, including
2 on the high value assets of the agency; or

3 “(B) coordinate with the Director of the
4 Cybersecurity and Infrastructure Security
5 Agency to ensure that penetration testing is
6 being performed;

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

9 “(A) adverse impacts to the operations of
10 the agency;

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

13 “(C) inappropriate access to data;

14 “(3) require the results of penetration testing
15 to include feedback to improve the cybersecurity of
16 the agency; and

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

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

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

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

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

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

12 “(e) RESPONSIBILITIES OF OMB.—The Director, in
13 coordination with the Director of the Cybersecurity and
14 Infrastructure Security Agency, shall—

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

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

19 “(f) PRIORITIZATION OF PENETRATION TESTING RE-
20 SOURCES.—

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

1 “(2) CONSIDERATIONS.—In developing the
2 framework under this subsection, the Director shall
3 consider—

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

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

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

10 “(D) any other information determined ap-
11 propriate by the Director or the Director of the
12 Cybersecurity and Infrastructure Security
13 Agency.

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

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

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

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

24 (b) DEADLINE FOR GUIDANCE.—Not later than 180
25 days after the date of enactment of this Act, the Director

1 shall issue the guidance required under section 3559A(b)
 2 of title 44, United States Code, as added by subsection
 3 (a).

4 (c) 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 3559 the fol-
 7 lowing:

“3559A. Federal penetration testing.”.

8 (d) SUNSET.—

9 (1) IN GENERAL.—Effective on the date that is
 10 10 years after the date of enactment of this Act,
 11 subchapter II of chapter 35 of title 44, United
 12 States Code, is amended by striking section 3559A.

13 (2) CLERICAL AMENDMENT.—Effective on the
 14 date that is 10 years after the date of enactment of
 15 this Act, the table of sections for chapter 35 of title
 16 44, United States Code, is amended by striking the
 17 item relating to section 3559A.

18 **SEC. 112. ONGOING THREAT HUNTING PROGRAM.**

19 (a) THREAT HUNTING PROGRAM.—

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

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

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

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

13 (C) staff threat hunting services;

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

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

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

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

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

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

9 (2) not less than 30 days before the date on
10 which the Director of the Cybersecurity and Infra-
11 structure Security Agency begins providing threat
12 hunting services under the program under sub-
13 section (a)(1), a report providing any updates to the
14 plan developed under subsection (a)(2); and

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

1 **SEC. 113. CODIFYING VULNERABILITY DISCLOSURE PRO-**
 2 **GRAMS.**

3 (a) IN GENERAL.—Chapter 35 of title 44, United
 4 States Code, is amended by inserting after section 3559A,
 5 as added by section 111 of this title, the following:

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

7 “(a) PURPOSE; SENSE OF CONGRESS.—

8 “(1) PURPOSE.—The purpose of Federal vul-
 9 nerability disclosure programs is to create a mecha-
 10 nism to use the expertise of the public to provide a
 11 service to Federal agencies by identifying informa-
 12 tion system vulnerabilities.

13 “(2) SENSE OF CONGRESS.—It is the sense of
 14 Congress that, in implementing the requirements of
 15 this section, the Federal Government should take
 16 appropriate steps to reduce real and perceived bur-
 17 dens in communications between agencies and secu-
 18 rity researchers.

19 “(b) DEFINITIONS.—In this section:

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

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

1 “(c) RESPONSIBILITIES OF OMB.—

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

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

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

14 “(2) SHARING INFORMATION WITH CISA.—The
15 Director, in coordination with the Director of the
16 Cybersecurity and Infrastructure Security Agency
17 and in consultation with the National Cyber Direc-
18 tor, shall issue guidance to agencies on sharing rel-
19 evant information in a consistent, automated, and
20 machine readable manner with the Director of the
21 Cybersecurity and Infrastructure Security Agency,
22 including—

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

1 mation systems that use commercial software or
2 services;

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

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

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

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

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

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

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

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

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

14 “(e) RESPONSIBILITIES OF AGENCIES.—

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

19 “(A) an appropriate security contact; and

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

23 “(2) VULNERABILITY DISCLOSURE POLICY.—

24 The head of each agency shall develop and make

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

3 “(A) describe—

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

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

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

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

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

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

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

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

24 “(D) be mature in scope and cover every
25 internet accessible Federal information system

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

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

8 “(f) CONGRESSIONAL REPORTING.—Not later than
9 90 days after the date of enactment of the Federal Infor-
10 mation Security Modernization Act of 2022, and annually
11 thereafter for a 3-year period, the Director of the Cyberse-
12 curity and Infrastructure Security Agency, in consultation
13 with the Director, shall provide to the Committee on
14 Homeland Security and Governmental Affairs of the Sen-
15 ate and the Committee on Oversight and Reform of the
16 House of Representatives a briefing on the status of the
17 use of vulnerability disclosure policies under this section
18 at agencies, including, with respect to the guidance issued
19 under subsection (c)(3), an identification of the agencies
20 that are compliant and not compliant.

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

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

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

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

10 (b) CLERICAL AMENDMENT.—The table of sections
11 for chapter 35 of title 44, United States Code, is amended
12 by adding after the item relating to section 3559A, as
13 added by section 111, the following:

“3559B. Federal vulnerability disclosure programs.”.

14 (c) SUNSET.—

15 (1) IN GENERAL.—Effective on the date that is
16 10 years after the date of enactment of this Act,
17 subchapter II of chapter 35 of title 44, United
18 States Code, is amended by striking section 3559B.

19 (2) CLERICAL AMENDMENT.—Effective on the
20 date that is 10 years after the date of enactment of
21 this Act, the table of sections for chapter 35 of title
22 44, United States Code, is amended by striking the
23 item relating to section 3559B.

1 **SEC. 114. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

2 (a) GUIDANCE.—Not later than 18 months after the
3 date of enactment of this Act, the Director shall provide
4 an update to the appropriate congressional committees on
5 progress in increasing the internal defenses of agency sys-
6 tems, including—

7 (1) shifting away from “trusted networks” to
8 implement security controls based on a presumption
9 of compromise;

10 (2) implementing principles of least privilege in
11 administering information security programs;

12 (3) limiting the ability of entities that cause in-
13 cidents to move laterally through or between agency
14 systems;

15 (4) identifying incidents quickly;

16 (5) isolating and removing unauthorized entities
17 from agency systems as quickly as practicable, ac-
18 counting for intelligence or law enforcement pur-
19 poses;

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

22 (7) a summary of the agency progress reports
23 required under subsection (b).

24 (b) AGENCY PROGRESS REPORTS.—Not later than
25 270 days after the date of enactment of this Act, the head
26 of each agency shall submit to the Director a progress re-

1 port on implementing an information security program
2 based on the presumption of compromise and least privi-
3 lege principles, which shall include—

4 (1) a description of any steps the agency has
5 completed, including progress toward achieving re-
6 quirements issued by the Director, including the
7 adoption of any models or reference architecture;

8 (2) an identification of activities that have not
9 yet been completed and that would have the most
10 immediate security impact; and

11 (3) a schedule to implement any planned activi-
12 ties.

13 **SEC. 115. AUTOMATION REPORTS.**

14 (a) OMB REPORT.—Not later than 180 days after
15 the date of enactment of this Act, the Director shall pro-
16 vide to the appropriate congressional committees an up-
17 date on the use of automation under paragraphs (1),
18 (5)(C), and (8)(B) of section 3554(b) of title 44, United
19 States Code.

20 (b) GAO REPORT.—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 on the use of
23 automation and machine readable data across the Federal
24 Government for cybersecurity purposes, including the

1 automated updating of cybersecurity tools, sensors, or
2 processes by agencies.

3 **SEC. 116. EXTENSION OF FEDERAL ACQUISITION SECURITY**

4 **COUNCIL AND SOFTWARE INVENTORY.**

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

8 (b) **REQUIREMENT.**—Subsection 1326(b) of title 41,
9 United States Code, is amended—

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

12 (2) by redesignating paragraph (6) as para-
13 graph (7); and

14 (3) by inserting after paragraph (5) the fol-
15 lowing:

16 “(6) maintaining an up-to-date and accurate in-
17 ventory of software in use by the agency and, if
18 available and applicable, the components of such
19 software, that can be communicated at the request
20 of the Federal Acquisition Security Council, the Na-
21 tional Cyber Director, or the Secretary of Homeland
22 Security, acting through the Director of Cybersecu-
23 rity and Infrastructure Security Agency; and”.

1 **SEC. 117. COUNCIL OF THE INSPECTORS GENERAL ON IN-**
2 **TEGRITY AND EFFICIENCY DASHBOARD.**

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

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

8 (2) by redesignating subparagraph (B) as sub-
9 paragraph (C); and

10 (3) by inserting after subparagraph (A) the fol-
11 lowing:

12 “(B) that shall include a dashboard of
13 open information security recommendations
14 identified in the independent evaluations re-
15 quired by section 3555(a) of title 44, United
16 States Code; and”.

17 **SEC. 118. QUANTITATIVE CYBERSECURITY METRICS.**

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

22 (b) UPDATING AND ESTABLISHING METRICS.—Not
23 later than 1 year after the date of enactment of this Act,
24 and as appropriate thereafter, the Director of the Cyberse-
25 curity and Infrastructure Security Agency, in coordination
26 with the Director, shall—

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

3 (2) as appropriate and pursuant to section
4 224(c) of the Cybersecurity Act of 2015 (6 U.S.C.
5 1522(c)) update or establish new covered metrics.

6 (c) IMPLEMENTATION.—

7 (1) IN GENERAL.—Not later than 540 days
8 after the date of enactment of this Act, the Director,
9 in coordination with the Director of the Cybersecu-
10 rity and Infrastructure Security Agency, shall pro-
11 mulgate guidance that requires each agency to use
12 covered metrics to track trends in the cybersecurity
13 and incident response capabilities of the agency.

14 (2) PERFORMANCE DEMONSTRATION.—The
15 guidance issued under paragraph (1) and any subse-
16 quent guidance shall require agencies to share with
17 the Director of the Cybersecurity and Infrastructure
18 Security Agency data demonstrating the perform-
19 ance of the agency using the covered metrics in-
20 cluded in the guidance.

21 (3) PENETRATION TESTS.—On not less than 2
22 occasions during the 2-year period following the date
23 on which guidance is promulgated under paragraph
24 (1), the Director shall ensure that not less than 3
25 agencies are subjected to substantially similar pene-

1 tration tests, as determined by the Director, in co-
2 ordination with the Director of the Cybersecurity
3 and Infrastructure Security Agency, in order to vali-
4 date the utility of the covered metrics.

5 (4) ANALYSIS CAPACITY.—The Director of the
6 Cybersecurity and Infrastructure Security Agency
7 shall develop a capability that allows for the analysis
8 of the covered metrics, including cross-agency per-
9 formance of agency cybersecurity and incident re-
10 sponse capability trends.

11 (5) TIME-BASED METRIC.—With respect the
12 first update or establishment of covered metrics re-
13 quired under subsection (b)(2), the Director of the
14 Cybersecurity and Infrastructure Security Agency
15 shall establish covered metrics that include not less
16 than 1 metric addressing the time it takes for agen-
17 cies to identify and respond to incidents.

18 (d) CONGRESSIONAL REPORTS.—Not later than 1
19 year after the date of enactment of this Act, the Director
20 of the Cybersecurity and Infrastructure Security Agency,
21 in coordination with the Director, shall submit to the ap-
22 propriate congressional committees a report on the utility
23 and use of the covered metrics.

1 **SEC. 119. ESTABLISHMENT OF RISK-BASED BUDGET**
2 **MODEL.**

3 (a) DEFINITIONS.—In this section:

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

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

10 (B) the Committee on Oversight and Re-
11 form, the Committee on Homeland Security,
12 and the Committee on Appropriations of the
13 House of Representatives.

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

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

21 (4) INFORMATION TECHNOLOGY.—The term
22 “information technology”—

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

25 (B) includes the hardware and software
26 systems of a Federal agency that monitor and

1 control physical equipment and processes of the
2 Federal agency.

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

5 (A) developed by identifying and
6 prioritizing cybersecurity risks and
7 vulnerabilities, including impact on agency oper-
8 ations in the case of a cyber attack, through
9 analysis of cyber threat intelligence, incident
10 data, and tactics, techniques, procedures, and
11 capabilities of cyber threats; and

12 (B) that allocates resources based on the
13 risks identified and prioritized under subpara-
14 graph (A).

15 (b) ESTABLISHMENT OF RISK-BASED BUDGET
16 MODEL.—

17 (1) IN GENERAL.—

18 (A) MODEL.—Not later than 1 year after
19 the first publication of the budget submitted by
20 the President under section 1105 of title 31,
21 United States Code, following the date of enact-
22 ment of this Act, the Director, in consultation
23 with the Director of the Cybersecurity and In-
24 frastructure Security Agency and the National
25 Cyber Director and in coordination with the Di-

1 rector of the National Institute of Standards
2 and Technology, shall develop a standard model
3 for informing a risk-based budget for cybersecu-
4 rity spending.

5 (B) RESPONSIBILITY OF DIRECTOR.—Sec-
6 tion 3553(a) of title 44, United States Code, as
7 amended by section 103 of this title, is further
8 amended by inserting after paragraph (6) the
9 following:

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

13 (C) CONTENTS OF MODEL.—The model re-
14 quired to be developed under subparagraph (A)
15 shall utilize appropriate information to evaluate
16 risk, including, as determined appropriate by
17 the Director—

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

22 (ii) analysis of the impact of agency
23 operations of compromise of systems, in-
24 cluding the interconnectivity to other agen-

cy systems and the operations of other agencies; and

(iii) to the greatest extent practicable, analysis of where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities.

(D) USE OF MODEL.—The model required to be developed under subparagraph (A) shall be used to—

(i) inform acquisition and sustainment of—

(I) information technology and cybersecurity tools;

(II) information technology and cybersecurity architectures;

(III) information technology and cybersecurity personnel; and

(IV) cybersecurity and information technology concepts of operations; and

(ii) evaluate and inform Government-wide cybersecurity programs.

(E) MODEL VARIATION.—The Director may develop multiple models under subpara-

graph (A) based on different agency characteristics, such as size or cybersecurity maturity.

(F) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under subparagraph (A).

(G) PUBLICATION.—Not earlier than 5 years after the date on which the model developed under subparagraph (A) is completed, the Director shall, taking into account any classified or sensitive information, publish the model, and any updates necessary under subparagraph (F), on the public website of the Office of Management and Budget.

(H) REPORTS.—Not later than 2 years after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under subparagraph (A) is completed, whichever is sooner, the Director shall submit to the appropriate congressional com-

1 mittees a report on the development of the
2 model.

3 (2) PHASED IMPLEMENTATION OF RISK-BASED
4 BUDGET MODEL.—

5 (A) INITIAL PHASE.—

6 (i) IN GENERAL.—Not later than 2
7 years after the date on which the model
8 developed under paragraph (1) is com-
9 pleted, the Director shall require not less
10 than 5 covered agencies to use the model
11 to inform the development of the annual
12 cybersecurity and information technology
13 budget requests of those covered agencies.

14 (ii) BRIEFING.—Not later than 1 year
15 after the date on which the covered agen-
16 cies selected under clause (i) begin using
17 the model developed under paragraph (1),
18 the Director shall provide to the appro-
19 priate congressional committees a briefing
20 on implementation of risk-based budgeting
21 for cybersecurity spending, an assessment
22 of agency implementation, and an evalua-
23 tion of whether the risk-based budget helps
24 to mitigate cybersecurity vulnerabilities.

1 (B) FULL DEPLOYMENT.—Not later than
2 5 years after the date on which the model devel-
3 oped under paragraph (1) is completed, the
4 head of each covered agency shall use the
5 model, or any updated model pursuant to para-
6 graph (1)(F), to the greatest extent practicable,
7 to inform the development of the annual cyber-
8 security and information technology budget re-
9 quests of the covered agency.

10 (C) AGENCY PERFORMANCE PLANS.—

11 (i) AMENDMENT.—Section 3554(d)(2)
12 of title 44, United States Code, is amended
13 by inserting “and the risk-based budget
14 model required under section 3553(a)(7)”
15 after “paragraph (1)”.

16 (ii) EFFECTIVE DATE.—The amend-
17 ment made by clause (i) shall take effect
18 on the date that is 5 years after the date
19 on which the model developed under para-
20 graph (1) is completed.

21 (3) VERIFICATION.—

22 (A) IN GENERAL.—Section
23 1105(a)(35)(A)(i) of title 31, United States
24 Code, is amended—

1 (i) in the matter preceding subclause
2 (I), by striking “by agency, and by initia-
3 tive area (as determined by the administra-
4 tion)” and inserting “and by agency”;

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

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

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

12 “(VI) a report on the progress of
13 each agency on closing recommenda-
14 tions identified under the independent
15 evaluation required by section
16 3555(a)(1) of title 44.”.

17 (B) EFFECTIVE DATE.—The amendments
18 made by subparagraph (A) shall take effect on
19 the date that is 5 years after the date on which
20 the model developed under paragraph (1) is
21 completed.

22 (4) REPORTS.—

23 (A) INDEPENDENT EVALUATION.—Section
24 3555(a)(2) of title 44, United States Code, is
25 amended—

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

3 (ii) in subparagraph (C), by striking
4 the period at the end and inserting “;
5 and”; and

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

8 “(D) an assessment of how the agency was
9 informed by the risk-based budget model re-
10 quired under section 3553(a)(7) and an evalua-
11 tion of whether the model mitigates agency
12 cyber vulnerabilities.”.

13 (B) ASSESSMENT.—

14 (i) AMENDMENT.—Section 3553(e) of
15 title 44, United States Code, as amended
16 by section 103 of this title, is further
17 amended by inserting after paragraph (5)
18 the following:

19 “(6) an assessment of—

20 “(A) Federal agency utilization of the
21 model required under subsection (a)(7); and

22 “(B) whether the model mitigates the
23 cyber vulnerabilities of the Federal Govern-
24 ment.”.

1 (ii) EFFECTIVE DATE.—The amend-
2 ment made by clause (i) shall take effect
3 on the date that is 5 years after the date
4 on which the model developed under para-
5 graph (1) is completed.

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

14 (A) an evaluation of the success of covered
15 agencies in utilizing the risk-based budget
16 model;

17 (B) an evaluation of the success of covered
18 agencies in implementing risk-based budgets;

19 (C) an evaluation of whether the risk-based
20 budgets developed by covered agencies are effec-
21 tive at informing Federal Government-wide cy-
22 bersecurity programs; and

23 (D) any other information relating to risk-
24 based budgets the Comptroller General deter-
25 mines appropriate.

1 **SEC. 120. 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 and the National Cyber Director, shall per-
16 form a study on the use of active defense techniques to
17 enhance the security of agencies, 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 agency operations and mission delivery, threat re-
9 sponse efforts, criminal investigations, and national
10 security activities, including intelligence collection;
11 and

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

14 **SEC. 121. SECURITY OPERATIONS CENTER AS A SERVICE**
15 **PILOT.**

16 (a) PURPOSE.—The purpose of this section is for the
17 Cybersecurity and Infrastructure Security Agency to run
18 a security operation center on behalf of another agency,
19 alleviating the need to duplicate this function at every
20 agency, and empowering a greater centralized cybersecu-
21 rity capability.

22 (b) PLAN.—Not later than 1 year after the date of
23 enactment of this Act, the Director of the Cybersecurity
24 and Infrastructure Security Agency shall develop a plan
25 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 270 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).

23 **SEC. 122. EXTENSION OF CHIEF DATA OFFICER COUNCIL.**

24 Section 3520A(e)(2) of title 44, United States Code,
 25 is amended by striking “upon the expiration of the 2-year

1 period that begins on the date the Comptroller General
 2 submits the report under paragraph (1) to Congress” and
 3 inserting “January 31, 2030”.

4 **TITLE II—CYBER INCIDENT RE-**
 5 **PORTING FOR CRITICAL IN-**
 6 **FRASTRUCTURE ACT OF 2022**

7 **SEC. 201. SHORT TITLE.**

8 This title may be cited as the “Cyber Incident Re-
 9 porting for Critical Infrastructure Act of 2022”.

10 **SEC. 202. DEFINITIONS.**

11 In this title:

12 (1) COVERED CYBER INCIDENT; COVERED ENTI-
 13 TY; CYBER INCIDENT; INFORMATION SYSTEM; RAN-
 14 SOM PAYMENT; RANSOMWARE ATTACK; SECURITY
 15 VULNERABILITY.—The terms “covered cyber inci-
 16 dent”, “covered entity”, “cyber incident”, “informa-
 17 tion system”, “ransom payment”, “ransomware at-
 18 tack”, and “security vulnerability” have the mean-
 19 ings given those terms in section 2240 of the Home-
 20 land Security Act of 2002, as added by section 203
 21 of this title.

22 (2) DIRECTOR.—The term “Director” means
 23 the Director of the Cybersecurity and Infrastructure
 24 Security Agency.

1 **SEC. 203. CYBER INCIDENT REPORTING.**

2 (a) CYBER INCIDENT REPORTING.—Title XXII of
3 the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
4 is amended—

5 (1) in section 2209(c) (6 U.S.C. 659(c))—

6 (A) in paragraph (11), by striking “; and”
7 and inserting a semicolon;

8 (B) in paragraph (12), by striking the pe-
9 riod at the end and inserting “; and”; and

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

11 “(13) receiving, aggregating, and analyzing re-
12 ports related to covered cyber incidents (as defined
13 in section 2240) submitted by covered entities (as
14 defined in section 2240) and reports related to ran-
15 som payments (as defined in section 2240) sub-
16 mitted by covered entities (as defined in section
17 2240) in furtherance of the activities specified in
18 sections 2202(e), 2203, and 2241, this subsection,
19 and any other authorized activity of the Director, to
20 enhance the situational awareness of cybersecurity
21 threats across critical infrastructure sectors.”; and

22 (2) by adding at the end the following:

23 **“Subtitle D—Cyber Incident**
24 **Reporting**

25 **“SEC. 2240. DEFINITIONS.**

26 “In this subtitle:

1 “(1) CENTER.—The term ‘Center’ means the
2 center established under section 2209.

3 “(2) CLOUD SERVICE PROVIDER.—The term
4 ‘cloud service provider’ means an entity offering
5 products or services related to cloud computing, as
6 defined by the National Institute of Standards and
7 Technology in NIST Special Publication 800–145
8 and any amendatory or superseding document relat-
9 ing thereto.

10 “(3) COUNCIL.—The term ‘Council’ means the
11 Cyber Incident Reporting Council described in sec-
12 tion 2246.

13 “(4) COVERED CYBER INCIDENT.—The term
14 ‘covered cyber incident’ means a substantial cyber
15 incident experienced by a covered entity that satis-
16 fies the definition and criteria established by the Di-
17 rector in the final rule issued pursuant to section
18 2242(b).

19 “(5) COVERED ENTITY.—The term ‘covered en-
20 tity’ means an entity in a critical infrastructure sec-
21 tor, as defined in Presidential Policy Directive 21,
22 that satisfies the definition established by the Direc-
23 tor in the final rule issued pursuant to section
24 2242(b).

1 “(6) CYBER INCIDENT.—The term ‘cyber inci-
2 dent’—

3 “(A) has the meaning given the term ‘inci-
4 dent’ in section 2209; and

5 “(B) does not include an occurrence that
6 imminently, but not actually, jeopardizes—

7 “(i) information on information sys-
8 tems; or

9 “(ii) information systems.

10 “(7) CYBER THREAT.—The term ‘cyber threat’
11 has the meaning given the term ‘cybersecurity
12 threat’ in section 2201.

13 “(8) CYBER THREAT INDICATOR; CYBERSECU-
14 RITY PURPOSE; DEFENSIVE MEASURE; FEDERAL EN-
15 TITY; SECURITY VULNERABILITY.—The terms ‘cyber
16 threat indicator’, ‘cybersecurity purpose’, ‘defensive
17 measure’, ‘Federal entity’, and ‘security vulner-
18 ability’ have the meanings given those terms in sec-
19 tion 102 of the Cybersecurity Act of 2015 (6 U.S.C.
20 1501).

21 “(9) INCIDENT; SHARING.—The terms ‘inci-
22 dent’ and ‘sharing’ have the meanings given those
23 terms in section 2209.

24 “(10) INFORMATION SHARING AND ANALYSIS
25 ORGANIZATION.—The term ‘Information Sharing

1 and Analysis Organization’ has the meaning given
2 the term in section 2222.

3 “(11) INFORMATION SYSTEM.—The term ‘infor-
4 mation system’—

5 “(A) has the meaning given the term in
6 section 3502 of title 44, United States Code;
7 and

8 “(B) includes industrial control systems,
9 such as supervisory control and data acquisition
10 systems, distributed control systems, and pro-
11 grammable logic controllers.

12 “(12) MANAGED SERVICE PROVIDER.—The
13 term ‘managed service provider’ means an entity
14 that delivers services, such as network, application,
15 infrastructure, or security services, via ongoing and
16 regular support and active administration on the
17 premises of a customer, in the data center of the en-
18 tity (such as hosting), or in a third party data cen-
19 ter.

20 “(13) RANSOM PAYMENT.—The term ‘ransom
21 payment’ means the transmission of any money or
22 other property or asset, including virtual currency,
23 or any portion thereof, which has at any time been
24 delivered as ransom in connection with a
25 ransomware attack.

1 “(14) RANSOMWARE ATTACK.—The term
2 ‘ransomware attack’—

3 “(A) means an incident that includes the
4 use or threat of use of unauthorized or mali-
5 cious code on an information system, or the use
6 or threat of use of another digital mechanism
7 such as a denial of service attack, to interrupt
8 or disrupt the operations of an information sys-
9 tem or compromise the confidentiality, avail-
10 ability, or integrity of electronic data stored on,
11 processed by, or transiting an information sys-
12 tem to extort a demand for a ransom payment;
13 and

14 “(B) does not include any such event
15 where the demand for payment is—

16 “(i) not genuine; or

17 “(ii) made in good faith by an entity
18 in response to a specific request by the
19 owner or operator of the information sys-
20 tem.

21 “(15) SECTOR RISK MANAGEMENT AGENCY.—
22 The term ‘Sector Risk Management Agency’ has the
23 meaning given the term in section 2201.

24 “(16) SIGNIFICANT CYBER INCIDENT.—The
25 term ‘significant cyber incident’ means a cyber inci-

1 dent, or a group of related cyber incidents, that the
 2 Secretary determines is likely to result in demon-
 3 strable harm to the national security interests, for-
 4 eign relations, or economy of the United States or
 5 to the public confidence, civil liberties, or public
 6 health and safety of the people of the United States.

7 “(17) SUPPLY CHAIN COMPROMISE.—The term
 8 ‘supply chain compromise’ means an incident within
 9 the supply chain of an information system that an
 10 adversary can leverage or does leverage to jeopardize
 11 the confidentiality, integrity, or availability of the in-
 12 formation system or the information the system
 13 processes, stores, or transmits, and can occur at any
 14 point during the life cycle.

15 “(18) VIRTUAL CURRENCY.—The term ‘virtual
 16 currency’ means the digital representation of value
 17 that functions as a medium of exchange, a unit of
 18 account, or a store of value.

19 “(19) VIRTUAL CURRENCY ADDRESS.—The
 20 term ‘virtual currency address’ means a unique pub-
 21 lic cryptographic key identifying the location to
 22 which a virtual currency payment can be made.

23 **“SEC. 2241. CYBER INCIDENT REVIEW.**

24 “(a) ACTIVITIES.—The Center shall—

1 “(1) receive, aggregate, analyze, and secure,
2 using processes consistent with the processes devel-
3 oped pursuant to the Cybersecurity Information
4 Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports
5 from covered entities related to a covered cyber inci-
6 dent to assess the effectiveness of security controls,
7 identify tactics, techniques, and procedures adver-
8 saries use to overcome those controls and other cy-
9 bersecurity purposes, including to assess potential
10 impact of cyber incidents on public health and safety
11 and to enhance situational awareness of cyber
12 threats across critical infrastructure sectors;

13 “(2) coordinate and share information with ap-
14 propriate Federal departments and agencies to iden-
15 tify and track ransom payments, including those uti-
16 lizing virtual currencies;

17 “(3) leverage information gathered about cyber
18 incidents to—

19 “(A) enhance the quality and effectiveness
20 of information sharing and coordination efforts
21 with appropriate entities, including agencies,
22 sector coordinating councils, Information Shar-
23 ing and Analysis Organizations, State, local,
24 Tribal, and territorial governments, technology
25 providers, critical infrastructure owners and op-

1 erators, cybersecurity and cyber incident re-
2 sponse firms, and security researchers; and

3 “(B) provide appropriate entities, including
4 sector coordinating councils, Information Shar-
5 ing and Analysis Organizations, State, local,
6 Tribal, and territorial governments, technology
7 providers, cybersecurity and cyber incident re-
8 sponse firms, and security researchers, with
9 timely, actionable, and anonymized reports of
10 cyber incident campaigns and trends, including,
11 to the maximum extent practicable, related con-
12 textual information, cyber threat indicators, and
13 defensive measures, pursuant to section 2245;

14 “(4) establish mechanisms to receive feedback
15 from stakeholders on how the Agency can most ef-
16 fectively receive covered cyber incident reports, ran-
17 som payment reports, and other voluntarily provided
18 information, and how the Agency can most effec-
19 tively support private sector cybersecurity;

20 “(5) facilitate the timely sharing, on a vol-
21 untary basis, between relevant critical infrastructure
22 owners and operators of information relating to cov-
23 ered cyber incidents and ransom payments, particu-
24 larly with respect to ongoing cyber threats or secu-
25 rity vulnerabilities and identify and disseminate

1 ways to prevent or mitigate similar cyber incidents
2 in the future;

3 “(6) for a covered cyber incident, including a
4 ransomware attack, that also satisfies the definition
5 of a significant cyber incident, or is part of a group
6 of related cyber incidents that together satisfy such
7 definition, conduct a review of the details sur-
8 rounding the covered cyber incident or group of
9 those incidents and identify and disseminate ways to
10 prevent or mitigate similar incidents in the future;

11 “(7) with respect to covered cyber incident re-
12 ports under section 2242(a) and 2243 involving an
13 ongoing cyber threat or security vulnerability, imme-
14 diately review those reports for cyber threat indica-
15 tors that can be anonymized and disseminated, with
16 defensive measures, to appropriate stakeholders, in
17 coordination with other divisions within the Agency,
18 as appropriate;

19 “(8) publish quarterly unclassified, public re-
20 ports that describe aggregated, anonymized observa-
21 tions, findings, and recommendations based on cov-
22 ered cyber incident reports, which may be based on
23 the unclassified information contained in the brief-
24 ings required under subsection (c);

1 “(9) proactively identify opportunities, con-
2 sistent with the protections in section 2245, to lever-
3 age and utilize data on cyber incidents in a manner
4 that enables and strengthens cybersecurity research
5 carried out by academic institutions and other pri-
6 vate sector organizations, to the greatest extent
7 practicable; and

8 “(10) in accordance with section 2245 and sub-
9 section (b) of this section, as soon as possible but
10 not later than 24 hours after receiving a covered
11 cyber incident report, ransom payment report, volun-
12 tarily submitted information pursuant to section
13 2243, or information received pursuant to a request
14 for information or subpoena under section 2244,
15 make available the information to appropriate Sector
16 Risk Management Agencies and other appropriate
17 Federal agencies.

18 “(b) INTERAGENCY SHARING.—The President or a
19 designee of the President—

20 “(1) may establish a specific time requirement
21 for sharing information under subsection (a)(11);
22 and

23 “(2) shall determine the appropriate Federal
24 agencies under subsection (a)(11).

1 “(c) PERIODIC BRIEFING.—Not later than 60 days
2 after the effective date of the final rule required under
3 section 2242(b), and on the first day of each month there-
4 after, the Director, in consultation with the National
5 Cyber Director, the Attorney General, and the Director
6 of National Intelligence, shall provide to the majority lead-
7 er of the Senate, the minority leader of the Senate, the
8 Speaker of the House of Representatives, the minority
9 leader of the House of Representatives, the Committee on
10 Homeland Security and Governmental Affairs of the Sen-
11 ate, and the Committee on Homeland Security of the
12 House of Representatives a briefing that characterizes the
13 national cyber threat landscape, including the threat fac-
14 ing Federal agencies and covered entities, and applicable
15 intelligence and law enforcement information, covered
16 cyber incidents, and ransomware attacks, as of the date
17 of the briefing, which shall—

18 “(1) include the total number of reports sub-
19 mitted under sections 2242 and 2243 during the
20 preceding month, including a breakdown of required
21 and voluntary reports;

22 “(2) include any identified trends in covered
23 cyber incidents and ransomware attacks over the
24 course of the preceding month and as compared to
25 previous reports, including any trends related to the

1 information collected in the reports submitted under
2 sections 2242 and 2243, including—

3 “(A) the infrastructure, tactics, and tech-
4 niques malicious cyber actors commonly use;
5 and

6 “(B) intelligence gaps that have impeded,
7 or currently are impeding, the ability to counter
8 covered cyber incidents and ransomware
9 threats;

10 “(3) include a summary of the known uses of
11 the information in reports submitted under sections
12 2242 and 2243; and

13 “(4) include an unclassified portion, but may
14 include a classified component.

15 **“SEC. 2242. REQUIRED REPORTING OF CERTAIN CYBER IN-**
16 **CIDENTS.**

17 “(a) IN GENERAL.—

18 “(1) COVERED CYBER INCIDENT REPORTS.—

19 “(A) IN GENERAL.—A covered entity that
20 experiences a covered cyber incident shall report
21 the covered cyber incident to the Agency not
22 later than 72 hours after the covered entity rea-
23 sonably believes that the covered cyber incident
24 has occurred.

1 “(B) LIMITATION.—The Director may not
2 require reporting under subparagraph (A) any
3 earlier than 72 hours after the covered entity
4 reasonably believes that a covered cyber inci-
5 dent has occurred.

6 “(2) RANSOM PAYMENT REPORTS.—

7 “(A) IN GENERAL.—A covered entity that
8 makes a ransom payment as the result of a
9 ransomware attack against the covered entity
10 shall report the payment to the Agency not
11 later than 24 hours after the ransom payment
12 has been made.

13 “(B) APPLICATION.—The requirements
14 under subparagraph (A) shall apply even if the
15 ransomware attack is not a covered cyber inci-
16 dent subject to the reporting requirements
17 under paragraph (1).

18 “(3) SUPPLEMENTAL REPORTS.—A covered en-
19 tity shall promptly submit to the Agency an update
20 or supplement to a previously submitted covered
21 cyber incident report if substantial new or different
22 information becomes available or if the covered enti-
23 ty makes a ransom payment after submitting a cov-
24 ered cyber incident report required under paragraph
25 (1), until such date that such covered entity notifies

1 the Agency that the covered cyber incident at issue
2 has concluded and has been fully mitigated and re-
3 solved.

4 “(4) PRESERVATION OF INFORMATION.—Any
5 covered entity subject to requirements of paragraph
6 (1), (2), or (3) shall preserve data relevant to the
7 covered cyber incident or ransom payment in accord-
8 ance with procedures established in the final rule
9 issued pursuant to subsection (b).

10 “(5) EXCEPTIONS.—

11 “(A) REPORTING OF COVERED CYBER IN-
12 CIDENT WITH RANSOM PAYMENT.—If a covered
13 entity is the victim of a covered cyber incident
14 and makes a ransom payment prior to the 72
15 hour requirement under paragraph (1), such
16 that the reporting requirements under para-
17 graphs (1) and (2) both apply, the covered enti-
18 ty may submit a single report to satisfy the re-
19 quirements of both paragraphs in accordance
20 with procedures established in the final rule
21 issued pursuant to subsection (b).

22 “(B) SUBSTANTIALLY SIMILAR REPORTED
23 INFORMATION.—

24 “(i) IN GENERAL.—Subject to the
25 limitation described in clause (ii), where

1 the Agency has an agreement in place that
2 satisfies the requirements of section 4(a) of
3 the Cyber Incident Reporting for Critical
4 Infrastructure Act of 2022, the require-
5 ments under paragraphs (1), (2), and (3)
6 shall not apply to a covered entity required
7 by law, regulation, or contract to report
8 substantially similar information to an-
9 other Federal agency within a substantially
10 similar timeframe.

11 “(ii) LIMITATION.—The exemption in
12 clause (i) shall take effect with respect to
13 a covered entity once an agency agreement
14 and sharing mechanism is in place between
15 the Agency and the respective Federal
16 agency, pursuant to section 4(a) of the
17 Cyber Incident Reporting for Critical In-
18 frastructure Act of 2022.

19 “(iii) RULES OF CONSTRUCTION.—
20 Nothing in this paragraph shall be con-
21 strued to—

22 “(I) exempt a covered entity
23 from the reporting requirements
24 under paragraph (3) unless the sup-
25 plemental report also meets the re-

1 quirements of clauses (i) and (ii) of
2 this paragraph;

3 “(II) prevent the Agency from
4 contacting an entity submitting infor-
5 mation to another Federal agency
6 that is provided to the Agency pursu-
7 ant to section 4 of the Cyber Incident
8 Reporting for Critical Infrastructure
9 Act of 2022; or

10 “(III) prevent an entity from
11 communicating with the Agency.

12 “(C) DOMAIN NAME SYSTEM.—The re-
13 quirements under paragraphs (1), (2) and (3)
14 shall not apply to a covered entity or the func-
15 tions of a covered entity that the Director de-
16 termines constitute critical infrastructure
17 owned, operated, or governed by multi-stake-
18 holder organizations that develop, implement,
19 and enforce policies concerning the Domain
20 Name System, such as the Internet Corporation
21 for Assigned Names and Numbers or the Inter-
22 net Assigned Numbers Authority.

23 “(6) MANNER, TIMING, AND FORM OF RE-
24 PORTS.—Reports made under paragraphs (1), (2),
25 and (3) shall be made in the manner and form, and

1 within the time period in the case of reports made
2 under paragraph (3), prescribed in the final rule
3 issued pursuant to subsection (b).

4 “(7) EFFECTIVE DATE.—Paragraphs (1)
5 through (4) shall take effect on the dates prescribed
6 in the final rule issued pursuant to subsection (b).

7 “(b) RULEMAKING.—

8 “(1) NOTICE OF PROPOSED RULEMAKING.—Not
9 later than 24 months after the date of enactment of
10 this section, the Director, in consultation with Sector
11 Risk Management Agencies, the Department of Jus-
12 tice, and other Federal agencies, shall publish in the
13 Federal Register a notice of proposed rulemaking to
14 implement subsection (a).

15 “(2) FINAL RULE.—Not later than 18 months
16 after publication of the notice of proposed rule-
17 making under paragraph (1), the Director shall
18 issue a final rule to implement subsection (a).

19 “(3) SUBSEQUENT RULEMAKINGS.—

20 “(A) IN GENERAL.—The Director is au-
21 thorized to issue regulations to amend or revise
22 the final rule issued pursuant to paragraph (2).

23 “(B) PROCEDURES.—Any subsequent rules
24 issued under subparagraph (A) shall comply
25 with the requirements under chapter 5 of title

1 5, United States Code, including the issuance of
2 a notice of proposed rulemaking under section
3 553 of such title.

4 “(c) ELEMENTS.—The final rule issued pursuant to
5 subsection (b) shall be composed of the following elements:

6 “(1) A clear description of the types of entities
7 that constitute covered entities, based on—

8 “(A) the consequences that disruption to
9 or compromise of such an entity could cause to
10 national security, economic security, or public
11 health and safety;

12 “(B) the likelihood that such an entity
13 may be targeted by a malicious cyber actor, in-
14 cluding a foreign country; and

15 “(C) the extent to which damage, disrup-
16 tion, or unauthorized access to such an entity,
17 including the accessing of sensitive cybersecu-
18 rity vulnerability information or penetration
19 testing tools or techniques, will likely enable the
20 disruption of the reliable operation of critical
21 infrastructure.

22 “(2) A clear description of the types of substan-
23 tial cyber incidents that constitute covered cyber in-
24 cidents, which shall—

1 “(A) at a minimum, require the occurrence
2 of—

3 “(i) a cyber incident that leads to sub-
4 stantial loss of confidentiality, integrity, or
5 availability of such information system or
6 network, or a serious impact on the safety
7 and resiliency of operational systems and
8 processes;

9 “(ii) a disruption of business or indus-
10 trial operations, including due to a denial
11 of service attack, ransomware attack, or
12 exploitation of a zero day vulnerability,
13 against

14 “(I) an information system or
15 network; or

16 “(II) an operational technology
17 system or process; or

18 “(iii) unauthorized access or disrup-
19 tion of business or industrial operations
20 due to loss of service facilitated through,
21 or caused by, a compromise of a cloud
22 service provider, managed service provider,
23 or other third-party data hosting provider
24 or by a supply chain compromise;

25 “(B) consider—

1 “(i) the sophistication or novelty of
2 the tactics used to perpetrate such a cyber
3 incident, as well as the type, volume, and
4 sensitivity of the data at issue;

5 “(ii) the number of individuals di-
6 rectly or indirectly affected or potentially
7 affected by such a cyber incident; and

8 “(iii) potential impacts on industrial
9 control systems, such as supervisory con-
10 trol and data acquisition systems, distrib-
11 uted control systems, and programmable
12 logic controllers; and

13 “(C) exclude—

14 “(i) any event where the cyber inci-
15 dent is perpetrated in good faith by an en-
16 tity in response to a specific request by the
17 owner or operator of the information sys-
18 tem; and

19 “(ii) the threat of disruption as extor-
20 tion, as described in section 2240(14)(A).

21 “(3) A requirement that, if a covered cyber inci-
22 dent or a ransom payment occurs following an ex-
23 empted threat described in paragraph (2)(C)(ii), the
24 covered entity shall comply with the requirements in

1 this subtitle in reporting the covered cyber incident
2 or ransom payment.

3 “(4) A clear description of the specific required
4 contents of a report pursuant to subsection (a)(1),
5 which shall include the following information, to the
6 extent applicable and available, with respect to a
7 covered cyber incident:

8 “(A) A description of the covered cyber in-
9 cident, including—

10 “(i) identification and a description of
11 the function of the affected information
12 systems, networks, or devices that were, or
13 are reasonably believed to have been, af-
14 fected by such cyber incident;

15 “(ii) a description of the unauthorized
16 access with substantial loss of confiden-
17 tiality, integrity, or availability of the af-
18 fected information system or network or
19 disruption of business or industrial oper-
20 ations;

21 “(iii) the estimated date range of such
22 incident; and

23 “(iv) the impact to the operations of
24 the covered entity.

1 “(B) Where applicable, a description of the
2 vulnerabilities exploited and the security de-
3 fenses that were in place, as well as the tactics,
4 techniques, and procedures used to perpetrate
5 the covered cyber incident.

6 “(C) Where applicable, any identifying or
7 contact information related to each actor rea-
8 sonably believed to be responsible for such cyber
9 incident.

10 “(D) Where applicable, identification of
11 the category or categories of information that
12 were, or are reasonably believed to have been,
13 accessed or acquired by an unauthorized per-
14 son.

15 “(E) The name and other information that
16 clearly identifies the covered entity impacted by
17 the covered cyber incident, including, as appli-
18 cable, the State of incorporation or formation of
19 the covered entity, trade names, legal names, or
20 other identifiers.

21 “(F) Contact information, such as tele-
22 phone number or electronic mail address, that
23 the Agency may use to contact the covered enti-
24 ty or an authorized agent of such covered enti-
25 ty, or, where applicable, the service provider of

1 such covered entity acting with the express per-
2 mission of, and at the direction of, the covered
3 entity to assist with compliance with the re-
4 quirements of this subtitle.

5 “(5) A clear description of the specific required
6 contents of a report pursuant to subsection (a)(2),
7 which shall be the following information, to the ex-
8 tent applicable and available, with respect to a ran-
9 som payment:

10 “(A) A description of the ransomware at-
11 tack, including the estimated date range of the
12 attack.

13 “(B) Where applicable, a description of the
14 vulnerabilities, tactics, techniques, and proce-
15 dures used to perpetrate the ransomware at-
16 tack.

17 “(C) Where applicable, any identifying or
18 contact information related to the actor or ac-
19 tors reasonably believed to be responsible for
20 the ransomware attack.

21 “(D) The name and other information that
22 clearly identifies the covered entity that made
23 the ransom payment or on whose behalf the
24 payment was made.

1 “(E) Contact information, such as tele-
2 phone number or electronic mail address, that
3 the Agency may use to contact the covered enti-
4 ty that made the ransom payment or an author-
5 ized agent of such covered entity, or, where ap-
6 plicable, the service provider of such covered en-
7 tity acting with the express permission of, and
8 at the direction of, that covered entity to assist
9 with compliance with the requirements of this
10 subtitle.

11 “(F) The date of the ransom payment.

12 “(G) The ransom payment demand, includ-
13 ing the type of virtual currency or other com-
14 modity requested, if applicable.

15 “(H) The ransom payment instructions,
16 including information regarding where to send
17 the payment, such as the virtual currency ad-
18 dress or physical address the funds were re-
19 quested to be sent to, if applicable.

20 “(I) The amount of the ransom payment.

21 “(6) A clear description of the types of data re-
22 quired to be preserved pursuant to subsection (a)(4),
23 the period of time for which the data is required to
24 be preserved, and allowable uses, processes, and pro-
25 cedures.

1 “(7) Deadlines and criteria for submitting sup-
2 plemental reports to the Agency required under sub-
3 section (a)(3), which shall—

4 “(A) be established by the Director in con-
5 sultation with the Council;

6 “(B) consider any existing regulatory re-
7 porting requirements similar in scope, purpose,
8 and timing to the reporting requirements to
9 which such a covered entity may also be sub-
10 ject, and make efforts to harmonize the timing
11 and contents of any such reports to the max-
12 imum extent practicable;

13 “(C) balance the need for situational
14 awareness with the ability of the covered entity
15 to conduct cyber incident response and inves-
16 tigations; and

17 “(D) provide a clear description of what
18 constitutes substantial new or different infor-
19 mation.

20 “(8) Procedures for—

21 “(A) entities, including third parties pur-
22 suant to subsection (d)(1), to submit reports re-
23 quired by paragraphs (1), (2), and (3) of sub-
24 section (a), including the manner and form

1 thereof, which shall include, at a minimum, a
2 concise, user-friendly web-based form;

3 “(B) the Agency to carry out—

4 “(i) the enforcement provisions of sec-
5 tion 2244, including with respect to the
6 issuance, service, withdrawal, referral proc-
7 ess, and enforcement of subpoenas, appeals
8 and due process procedures;

9 “(ii) other available enforcement
10 mechanisms including acquisition, suspen-
11 sion and debarment procedures; and

12 “(iii) other aspects of noncompliance;

13 “(C) implementing the exceptions provided
14 in subsection (a)(5); and

15 “(D) protecting privacy and civil liberties
16 consistent with processes adopted pursuant to
17 section 105(b) of the Cybersecurity Act of 2015
18 (6 U.S.C. 1504(b)) and anonymizing and safe-
19 guarding, or no longer retaining, information
20 received and disclosed through covered cyber in-
21 cident reports and ransom payment reports that
22 is known to be personal information of a spe-
23 cific individual or information that identifies a
24 specific individual that is not directly related to
25 a cybersecurity threat.

1 “(9) Other procedural measures directly nec-
2 essary to implement subsection (a).

3 “(d) THIRD PARTY REPORT SUBMISSION AND RAN-
4 SOM PAYMENT.—

5 “(1) REPORT SUBMISSION.—A covered entity
6 that is required to submit a covered cyber incident
7 report or a ransom payment report may use a third
8 party, such as an incident response company, insur-
9 ance provider, service provider, Information Sharing
10 and Analysis Organization, or law firm, to submit
11 the required report under subsection (a).

12 “(2) RANSOM PAYMENT.—If a covered entity
13 impacted by a ransomware attack uses a third party
14 to make a ransom payment, the third party shall not
15 be required to submit a ransom payment report for
16 itself under subsection (a)(2).

17 “(3) DUTY TO REPORT.—Third-party reporting
18 under this subparagraph does not relieve a covered
19 entity from the duty to comply with the require-
20 ments for covered cyber incident report or ransom
21 payment report submission.

22 “(4) RESPONSIBILITY TO ADVISE.—Any third
23 party used by a covered entity that knowingly makes
24 a ransom payment on behalf of a covered entity im-
25 pacted by a ransomware attack shall advise the im-

1 pacted covered entity of the responsibilities of the
2 impacted covered entity regarding reporting ransom
3 payments under this section.

4 “(e) OUTREACH TO COVERED ENTITIES.—

5 “(1) IN GENERAL.—The Agency shall conduct
6 an outreach and education campaign to inform likely
7 covered entities, entities that offer or advertise as a
8 service to customers to make or facilitate ransom
9 payments on behalf of covered entities impacted by
10 ransomware attacks and other appropriate entities
11 of the requirements of paragraphs (1), (2), and (3)
12 of subsection (a).

13 “(2) ELEMENTS.—The outreach and education
14 campaign under paragraph (1) shall include the fol-
15 lowing:

16 “(A) An overview of the final rule issued
17 pursuant to subsection (b).

18 “(B) An overview of mechanisms to submit
19 to the Agency covered cyber incident reports,
20 ransom payment reports, and information relat-
21 ing to the disclosure, retention, and use of cov-
22 ered cyber incident reports and ransom pay-
23 ment reports under this section.

24 “(C) An overview of the protections af-
25 forded to covered entities for complying with

1 the requirements under paragraphs (1), (2),
2 and (3) of subsection (a).

3 “(D) An overview of the steps taken under
4 section 2244 when a covered entity is not in
5 compliance with the reporting requirements
6 under subsection (a).

7 “(E) Specific outreach to cybersecurity
8 vendors, cyber incident response providers, cy-
9 bersecurity insurance entities, and other entities
10 that may support covered entities.

11 “(F) An overview of the privacy and civil
12 liberties requirements in this subtitle.

13 “(3) COORDINATION.—In conducting the out-
14 reach and education campaign required under para-
15 graph (1), the Agency may coordinate with—

16 “(A) the Critical Infrastructure Partner-
17 ship Advisory Council established under section
18 871;

19 “(B) Information Sharing and Analysis
20 Organizations;

21 “(C) trade associations;

22 “(D) information sharing and analysis cen-
23 ters;

24 “(E) sector coordinating councils; and

1 “(F) any other entity as determined appro-
 2 priate by the Director.

3 “(f) EXEMPTION.—Sections 3506(c), 3507, 3508,
 4 and 3509 of title 44, United States Code, shall not apply
 5 to any action to carry out this section.

6 “(g) RULE OF CONSTRUCTION.—Nothing in this sec-
 7 tion shall affect the authorities of the Federal Government
 8 to implement the requirements of Executive Order 14028
 9 (86 Fed. Reg. 26633; relating to improving the nation’s
 10 cybersecurity), including changes to the Federal Acquisi-
 11 tion Regulations and remedies to include suspension and
 12 debarment.

13 “(h) SAVINGS PROVISION.—Nothing in this section
 14 shall be construed to supersede or to abrogate, modify,
 15 or otherwise limit the authority that is vested in any offi-
 16 cer or any agency of the United States Government to reg-
 17 ulate or take action with respect to the cybersecurity of
 18 an entity.

19 **“SEC. 2243. VOLUNTARY REPORTING OF OTHER CYBER IN-**
 20 **CIDENTS.**

21 “(a) IN GENERAL.—Entities may voluntarily report
 22 cyber incidents or ransom payments to the Agency that
 23 are not required under paragraph (1), (2), or (3) of sec-
 24 tion 2242(a), but may enhance the situational awareness
 25 of cyber threats.

1 “(b) VOLUNTARY PROVISION OF ADDITIONAL INFOR-
2 MATION IN REQUIRED REPORTS.—Covered entities may
3 voluntarily include in reports required under paragraph
4 (1), (2), or (3) of section 2242(a) information that is not
5 required to be included, but may enhance the situational
6 awareness of cyber threats.

7 “(c) APPLICATION OF PROTECTIONS.—The protec-
8 tions under section 2245 applicable to reports made under
9 section 2242 shall apply in the same manner and to the
10 same extent to reports and information submitted under
11 subsections (a) and (b).

12 **“SEC. 2244. NONCOMPLIANCE WITH REQUIRED REPORTING.**

13 “(a) PURPOSE.—In the event that a covered entity
14 that is required to submit a report under section 2242(a)
15 fails to comply with the requirement to report, the Direc-
16 tor may obtain information about the cyber incident or
17 ransom payment by engaging the covered entity directly
18 to request information about the cyber incident or ransom
19 payment, and if the Director is unable to obtain informa-
20 tion through such engagement, by issuing a subpoena to
21 the covered entity, pursuant to subsection (c), to gather
22 information sufficient to determine whether a covered
23 cyber incident or ransom payment has occurred.

24 “(b) INITIAL REQUEST FOR INFORMATION.—

1 “(1) IN GENERAL.—If the Director has reason
2 to believe, whether through public reporting or other
3 information in the possession of the Federal Govern-
4 ment, including through analysis performed pursu-
5 ant to paragraph (1) or (2) of section 2241(a), that
6 a covered entity has experienced a covered cyber in-
7 cident or made a ransom payment but failed to re-
8 port such cyber incident or payment to the Agency
9 in accordance with section 2242(a), the Director
10 may request additional information from the covered
11 entity to confirm whether or not a covered cyber in-
12 cident or ransom payment has occurred.

13 “(2) TREATMENT.—Information provided to the
14 Agency in response to a request under paragraph
15 (1) shall be treated as if it was submitted through
16 the reporting procedures established in section 2242.

17 “(c) ENFORCEMENT.—

18 “(1) IN GENERAL.—If, after the date that is 72
19 hours from the date on which the Director made the
20 request for information in subsection (b), the Direc-
21 tor has received no response from the covered entity
22 from which such information was requested, or re-
23 ceived an inadequate response, the Director may
24 issue to such covered entity a subpoena to compel
25 disclosure of information the Director deems nec-

1 essary to determine whether a covered cyber incident
2 or ransom payment has occurred and obtain the in-
3 formation required to be reported pursuant to sec-
4 tion 2242 and any implementing regulations, and as-
5 sess potential impacts to national security, economic
6 security, or public health and safety.

7 “(2) CIVIL ACTION.—

8 “(A) IN GENERAL.—If a covered entity
9 fails to comply with a subpoena, the Director
10 may refer the matter to the Attorney General
11 to bring a civil action in a district court of the
12 United States to enforce such subpoena.

13 “(B) VENUE.—An action under this para-
14 graph may be brought in the judicial district in
15 which the covered entity against which the ac-
16 tion is brought resides, is found, or does busi-
17 ness.

18 “(C) CONTEMPT OF COURT.—A court may
19 punish a failure to comply with a subpoena
20 issued under this subsection as contempt of
21 court.

22 “(3) NON-DELEGATION.—The authority of the
23 Director to issue a subpoena under this subsection
24 may not be delegated.

25 “(4) AUTHENTICATION.—

1 “(A) IN GENERAL.—Any subpoena issued
2 electronically pursuant to this subsection shall
3 be authenticated with a cryptographic digital
4 signature of an authorized representative of the
5 Agency, or other comparable successor tech-
6 nology, that allows the Agency to demonstrate
7 that such subpoena was issued by the Agency
8 and has not been altered or modified since such
9 issuance.

10 “(B) INVALID IF NOT AUTHENTICATED.—
11 Any subpoena issued electronically pursuant to
12 this subsection that is not authenticated in ac-
13 cordance with subparagraph (A) shall not be
14 considered to be valid by the recipient of such
15 subpoena.

16 “(d) PROVISION OF CERTAIN INFORMATION TO AT-
17 TORNEY GENERAL.—

18 “(1) IN GENERAL.—Notwithstanding section
19 2245(a)(5) and paragraph (b)(2) of this section, if
20 the Director determines, based on the information
21 provided in response to a subpoena issued pursuant
22 to subsection (c), that the facts relating to the cyber
23 incident or ransom payment at issue may constitute
24 grounds for a regulatory enforcement action or
25 criminal prosecution, the Director may provide such

1 information to the Attorney General or the head of
2 the appropriate Federal regulatory agency, who may
3 use such information for a regulatory enforcement
4 action or criminal prosecution.

5 “(2) CONSULTATION.—The Director may con-
6 sult with the Attorney General or the head of the
7 appropriate Federal regulatory agency when making
8 the determination under paragraph (1).

9 “(e) CONSIDERATIONS.—When determining whether
10 to exercise the authorities provided under this section, the
11 Director shall take into consideration—

12 “(1) the complexity in determining if a covered
13 cyber incident has occurred; and

14 “(2) prior interaction with the Agency or
15 awareness of the covered entity of the policies and
16 procedures of the Agency for reporting covered cyber
17 incidents and ransom payments.

18 “(f) EXCLUSIONS.—This section shall not apply to a
19 State, local, Tribal, or territorial government entity.

20 “(g) REPORT TO CONGRESS.—The Director shall
21 submit to Congress an annual report on the number of
22 times the Director—

23 “(1) issued an initial request for information
24 pursuant to subsection (b);

1 “(2) issued a subpoena pursuant to subsection
2 (c); or

3 “(3) referred a matter to the Attorney General
4 for a civil action pursuant to subsection (c)(2).

5 “(h) PUBLICATION OF THE ANNUAL REPORT.—The
6 Director shall publish a version of the annual report re-
7 quired under subsection (g) on the website of the Agency,
8 which shall include, at a minimum, the number of times
9 the Director—

10 “(1) issued an initial request for information
11 pursuant to subsection (b); or

12 “(2) issued a subpoena pursuant to subsection
13 (c).

14 “(i) ANONYMIZATION OF REPORTS.—The Director
15 shall ensure any victim information contained in a report
16 required to be published under subsection (h) be
17 anonymized before the report is published.

18 **“SEC. 2245. INFORMATION SHARED WITH OR PROVIDED TO**
19 **THE FEDERAL GOVERNMENT.**

20 “(a) DISCLOSURE, RETENTION, AND USE.—

21 “(1) AUTHORIZED ACTIVITIES.—Information
22 provided to the Agency pursuant to section 2242 or
23 2243 may be disclosed to, retained by, and used by,
24 consistent with otherwise applicable provisions of
25 Federal law, any Federal agency or department,

1 component, officer, employee, or agent of the Fed-
2 eral Government solely for—

3 “(A) a cybersecurity purpose;

4 “(B) the purpose of identifying—

5 “(i) a cyber threat, including the
6 source of the cyber threat; or

7 “(ii) a security vulnerability;

8 “(C) the purpose of responding to, or oth-
9 erwise preventing or mitigating, a specific
10 threat of death, a specific threat of serious bod-
11 ily harm, or a specific threat of serious eco-
12 nomic harm, including a terrorist act or use of
13 a weapon of mass destruction;

14 “(D) the purpose of responding to, inves-
15 tigating, prosecuting, or otherwise preventing or
16 mitigating, a serious threat to a minor, includ-
17 ing sexual exploitation and threats to physical
18 safety; or

19 “(E) the purpose of preventing, inves-
20 tigating, disrupting, or prosecuting an offense
21 arising out of a cyber incident reported pursu-
22 ant to section 2242 or 2243 or any of the of-
23 fenses listed in section 105(d)(5)(A)(v) of the
24 Cybersecurity Act of 2015 (6 U.S.C.
25 1504(d)(5)(A)(v)).

1 “(2) AGENCY ACTIONS AFTER RECEIPT.—

2 “(A) RAPID, CONFIDENTIAL SHARING OF
3 CYBER THREAT INDICATORS.—Upon receiving a
4 covered cyber incident or ransom payment re-
5 port submitted pursuant to this section, the
6 Agency shall immediately review the report to
7 determine whether the cyber incident that is the
8 subject of the report is connected to an ongoing
9 cyber threat or security vulnerability and where
10 applicable, use such report to identify, develop,
11 and rapidly disseminate to appropriate stake-
12 holders actionable, anonymized cyber threat in-
13 dicators and defensive measures.

14 “(B) PRINCIPLES FOR SHARING SECURITY
15 VULNERABILITIES.—With respect to informa-
16 tion in a covered cyber incident or ransom pay-
17 ment report regarding a security vulnerability
18 referred to in paragraph (1)(B)(ii), the Director
19 shall develop principles that govern the timing
20 and manner in which information relating to se-
21 curity vulnerabilities may be shared, consistent
22 with common industry best practices and
23 United States and international standards.

24 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-
25 tion contained in covered cyber incident and ransom

1 payment reports submitted to the Agency pursuant
2 to section 2242 shall be retained, used, and dissemi-
3 nated, where permissible and appropriate, by the
4 Federal Government in accordance with processes to
5 be developed for the protection of personal informa-
6 tion consistent with processes adopted pursuant to
7 section 105 of the Cybersecurity Act of 2015 (6
8 U.S.C. 1504) and in a manner that protects from
9 unauthorized use or disclosure any information that
10 may contain—

11 “(A) personal information of a specific in-
12 dividual that is not directly related to a cyberse-
13 curity threat; or

14 “(B) information that identifies a specific
15 individual that is not directly related to a cyber-
16 security threat.

17 “(4) DIGITAL SECURITY.—The Agency shall en-
18 sure that reports submitted to the Agency pursuant
19 to section 2242, and any information contained in
20 those reports, are collected, stored, and protected at
21 a minimum in accordance with the requirements for
22 moderate impact Federal information systems, as
23 described in Federal Information Processing Stand-
24 ards Publication 199, or any successor document.

1 “(5) PROHIBITION ON USE OF INFORMATION IN
2 REGULATORY ACTIONS.—

3 “(A) IN GENERAL.—A Federal, State,
4 local, or Tribal government shall not use infor-
5 mation about a covered cyber incident or ran-
6 som payment obtained solely through reporting
7 directly to the Agency in accordance with this
8 subtitle to regulate, including through an en-
9 forcement action, the activities of the covered
10 entity or entity that made a ransom payment,
11 unless the government entity expressly allows
12 entities to submit reports to the Agency to meet
13 regulatory reporting obligations of the entity.

14 “(B) CLARIFICATION.—A report submitted
15 to the Agency pursuant to section 2242 or 2243
16 may, consistent with Federal or State regu-
17 latory authority specifically relating to the pre-
18 vention and mitigation of cybersecurity threats
19 to information systems, inform the development
20 or implementation of regulations relating to
21 such systems.

22 “(b) PROTECTIONS FOR REPORTING ENTITIES AND
23 INFORMATION.—Reports describing covered cyber inci-
24 dents or ransom payments submitted to the Agency by en-
25 tities in accordance with section 2242, as well as volun-

1 tarily-submitted cyber incident reports submitted to the
 2 Agency pursuant to section 2243, shall—

3 “(1) be considered the commercial, financial,
 4 and proprietary information of the covered entity
 5 when so designated by the covered entity;

6 “(2) be exempt from disclosure under section
 7 552(b)(3) of title 5, United States Code (commonly
 8 known as the ‘Freedom of Information Act’), as well
 9 as any provision of State, Tribal, or local freedom of
 10 information law, open government law, open meet-
 11 ings law, open records law, sunshine law, or similar
 12 law requiring disclosure of information or records;

13 “(3) be considered not to constitute a waiver of
 14 any applicable privilege or protection provided by
 15 law, including trade secret protection; and

16 “(4) not be subject to a rule of any Federal
 17 agency or department or any judicial doctrine re-
 18 garding ex parte communications with a decision-
 19 making official.

20 “(c) LIABILITY PROTECTIONS.—

21 “(1) IN GENERAL.—No cause of action shall lie
 22 or be maintained in any court by any person or enti-
 23 ty and any such action shall be promptly dismissed
 24 for the submission of a report pursuant to section
 25 2242(a) that is submitted in conformance with this

1 subtitle and the rule promulgated under section
2 2242(b), except that this subsection shall not apply
3 with regard to an action by the Federal Government
4 pursuant to section 2244(c)(2).

5 “(2) SCOPE.—The liability protections provided
6 in this subsection shall only apply to or affect litiga-
7 tion that is solely based on the submission of a cov-
8 ered cyber incident report or ransom payment report
9 to the Agency.

10 “(3) RESTRICTIONS.—Notwithstanding para-
11 graph (2), no report submitted to the Agency pursu-
12 ant to this subtitle or any communication, document,
13 material, or other record, created for the sole pur-
14 pose of preparing, drafting, or submitting such re-
15 port, may be received in evidence, subject to dis-
16 covery, or otherwise used in any trial, hearing, or
17 other proceeding in or before any court, regulatory
18 body, or other authority of the United States, a
19 State, or a political subdivision thereof, provided
20 that nothing in this subtitle shall create a defense to
21 discovery or otherwise affect the discovery of any
22 communication, document, material, or other record
23 not created for the sole purpose of preparing, draft-
24 ing, or submitting such report.

1 “(d) SHARING WITH NON-FEDERAL ENTITIES.—

2 The Agency shall anonymize the victim who reported the
3 information when making information provided in reports
4 received under section 2242 available to critical infrastruc-
5 ture owners and operators and the general public.

6 “(e) STORED COMMUNICATIONS ACT.—Nothing in
7 this subtitle shall be construed to permit or require disclo-
8 sure by a provider of a remote computing service or a pro-
9 vider of an electronic communication service to the public
10 of information not otherwise permitted or required to be
11 disclosed under chapter 121 of title 18, United States
12 Code (commonly known as the ‘Stored Communications
13 Act’).

14 **“SEC. 2246. CYBER INCIDENT REPORTING COUNCIL.**

15 “(a) RESPONSIBILITY OF THE SECRETARY.—The
16 Secretary shall lead an intergovernmental Cyber Incident
17 Reporting Council, in consultation with the Director of the
18 Office of Management and Budget, the Attorney General,
19 the National Director Cyber Director, Sector Risk Man-
20 agement Agencies, and other appropriate Federal agen-
21 cies, to coordinate, deconflict, and harmonize Federal inci-
22 dent reporting requirements, including those issued
23 through regulations.

1 “(b) RULE OF CONSTRUCTION.—Nothing in sub-
 2 section (a) shall be construed to provide any additional
 3 regulatory authority to any Federal entity.”.

4 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 5 The table of contents in section 1(b) of the Homeland Se-
 6 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)
 7 is amended by inserting after the items relating to subtitle
 8 C of title XXII the following:

“Subtitle D—Cyber Incident Reporting

“Sec. 2240. Definitions.

“Sec. 2241. Cyber Incident Review.

“Sec. 2242. Required reporting of certain cyber incidents.

“Sec. 2243. Voluntary reporting of other cyber incidents.

“Sec. 2244. Noncompliance with required reporting.

“Sec. 2245. Information shared with or provided to the Federal Government.

“Sec. 2246. Cyber Incident Reporting Council.”.

9 **SEC. 204. FEDERAL SHARING OF INCIDENT REPORTS.**

10 (a) CYBER INCIDENT REPORTING SHARING.—

11 (1) IN GENERAL.—Notwithstanding any other
 12 provision of law or regulation, any Federal agency,
 13 including any independent establishment (as defined
 14 in section 104 of title 5, United States Code), that
 15 receives a report from an entity of a cyber incident,
 16 including a ransomware attack, shall provide the re-
 17 port to the Agency as soon as possible, but not later
 18 than 24 hours after receiving the report, unless a
 19 shorter period is required by an agreement made be-
 20 tween the Department of Homeland Security (in-
 21 cluding the Cybersecurity and Infrastructure Secu-

1 rity Agency) and the recipient Federal agency. The
2 Director shall share and coordinate each report pur-
3 suant to section 2241(b) of the Homeland Security
4 Act of 2002, as added by section 203 of this title.

5 (2) RULE OF CONSTRUCTION.—The require-
6 ments described in paragraph (1) and section
7 2245(d) of the Homeland Security Act of 2002, as
8 added by section 203 of this title, may not be con-
9 strued to be a violation of any provision of law or
10 policy that would otherwise prohibit disclosure or
11 provision of information within the executive branch.

12 (3) PROTECTION OF INFORMATION.—The Di-
13 rector shall comply with any obligations of the re-
14 cipient Federal agency described in paragraph (1) to
15 protect information, including with respect to pri-
16 vacy, confidentiality, or information security, if those
17 obligations would impose greater protection require-
18 ments than this Act or the amendments made by
19 this Act.

20 (4) EFFECTIVE DATE.—This subsection shall
21 take effect on the effective date of the final rule
22 issued pursuant to section 2242(b) of the Homeland
23 Security Act of 2002, as added by section 203 of
24 this title.

25 (5) AGENCY AGREEMENTS.—

1 (A) IN GENERAL.—The Agency and any
2 Federal agency, including any independent es-
3 tablishment (as defined in section 104 of title
4 5, United States Code) that receives incident
5 reports from entities, including due to
6 ransomware attacks, shall, as appropriate, enter
7 into a documented agreement to establish poli-
8 cies, processes, procedures, and mechanisms to
9 ensure reports are shared with the Agency pur-
10 suant to paragraph (1).

11 (B) AVAILABILITY.—To the maximum ex-
12 tent practicable, each documented agreement
13 required under subparagraph (A) shall be made
14 publicly available.

15 (C) REQUIREMENT.—The documented
16 agreements required by subparagraph (A) shall
17 require reports be shared from Federal agencies
18 with the Agency in such time as to meet the
19 overall timeline for covered entity reporting of
20 covered cyber incidents and ransom payments
21 established in section 2242 of the Homeland
22 Security Act of 2002, as added by section 203
23 of this title.

24 (b) HARMONIZING REPORTING REQUIREMENTS.—
25 The Secretary of Homeland Security, acting through the

1 Director, shall, in consultation with the Cyber Incident
2 Reporting Council described in section 2246 of the Home-
3 land Security Act of 2002, as added by section 203 of
4 this title, to the maximum extent practicable—

5 (1) periodically review existing regulatory re-
6 quirements, including the information required in
7 such reports, to report incidents and ensure that any
8 such reporting requirements and procedures avoid
9 conflicting, duplicative, or burdensome requirements;
10 and

11 (2) coordinate with appropriate Federal part-
12 ners and regulatory authorities that receive reports
13 relating to incidents to identify opportunities to
14 streamline reporting processes, and where feasible,
15 facilitate interagency agreements between such au-
16 thorities to permit the sharing of such reports, con-
17 sistent with applicable law and policy, without im-
18 pacting the ability of the Agency to gain timely situ-
19 ational awareness of a covered cyber incident or ran-
20 som payment.

21 **SEC. 205. RANSOMWARE VULNERABILITY WARNING PILOT**
22 **PROGRAM.**

23 (a) PROGRAM.—Not later than 1 year after the date
24 of enactment of this Act, the Director shall establish a
25 ransomware vulnerability warning pilot program to lever-

1 age existing authorities and technology to specifically de-
2 velop processes and procedures for, and to dedicate re-
3 sources to, identifying information systems that contain
4 security vulnerabilities associated with common
5 ransomware attacks, and to notify the owners of those vul-
6 nerable systems of their security vulnerability.

7 (b) IDENTIFICATION OF VULNERABLE SYSTEMS.—
8 The pilot program established under subsection (a) shall—

9 (1) identify the most common security
10 vulnerabilities utilized in ransomware attacks and
11 mitigation techniques; and

12 (2) utilize existing authorities to identify infor-
13 mation systems that contain the security
14 vulnerabilities identified in paragraph (1).

15 (c) ENTITY NOTIFICATION.—

16 (1) IDENTIFICATION.—If the Director is able to
17 identify the entity at risk that owns or operates a
18 vulnerable information system identified in sub-
19 section (b), the Director may notify the owner of the
20 information system.

21 (2) NO IDENTIFICATION.—If the Director is not
22 able to identify the entity at risk that owns or oper-
23 ates a vulnerable information system identified in
24 subsection (b), the Director may utilize the subpoena
25 authority pursuant to section 2209 of the Homeland

1 Security Act of 2002 (6 U.S.C. 659) to identify and
2 notify the entity at risk pursuant to the procedures
3 under that section.

4 (3) REQUIRED INFORMATION.—A notification
5 made under paragraph (1) shall include information
6 on the identified security vulnerability and mitiga-
7 tion techniques.

8 (d) PRIORITIZATION OF NOTIFICATIONS.—To the ex-
9 tent practicable, the Director shall prioritize covered enti-
10 ties for identification and notification activities under the
11 pilot program established under this section.

12 (e) LIMITATION ON PROCEDURES.—No procedure,
13 notification, or other authorities utilized in the execution
14 of the pilot program established under subsection (a) shall
15 require an owner or operator of a vulnerable information
16 system to take any action as a result of a notice of a secu-
17 rity vulnerability made pursuant to subsection (c).

18 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
19 tion shall be construed to provide additional authorities
20 to the Director to identify vulnerabilities or vulnerable sys-
21 tems.

22 (g) TERMINATION.—The pilot program established
23 under subsection (a) shall terminate on the date that is
24 4 years after the date of enactment of this Act.

1 **SEC. 206. RANSOMWARE THREAT MITIGATION ACTIVITIES.**

2 (a) **JOINT RANSOMWARE TASK FORCE.**—

3 (1) **IN GENERAL.**—Not later than 180 days
4 after the date of enactment of this Act, the Director,
5 in consultation with the National Cyber Director,
6 the Attorney General, and the Director of the Fed-
7 eral Bureau of Investigation, shall establish and
8 chair the Joint Ransomware Task Force to coordi-
9 nate an ongoing nationwide campaign against
10 ransomware attacks, and identify and pursue oppor-
11 tunities for international cooperation.

12 (2) **COMPOSITION.**—The Joint Ransomware
13 Task Force shall consist of participants from Fed-
14 eral agencies, as determined appropriate by the Na-
15 tional Cyber Director in consultation with the Sec-
16 retary of Homeland Security.

17 (3) **RESPONSIBILITIES.**—The Joint
18 Ransomware Task Force, utilizing only existing au-
19 thorities of each participating Federal agency, shall
20 coordinate across the Federal Government the fol-
21 lowing activities:

22 (A) Prioritization of intelligence-driven op-
23 erations to disrupt specific ransomware actors.

24 (B) Consult with relevant private sector,
25 State, local, Tribal, and territorial governments
26 and international stakeholders to identify needs

1 and establish mechanisms for providing input
2 into the Joint Ransomware Task Force.

3 (C) Identifying, in consultation with rel-
4 evant entities, a list of highest threat
5 ransomware entities updated on an ongoing
6 basis, in order to facilitate—

7 (i) prioritization for Federal action by
8 appropriate Federal agencies; and

9 (ii) identify metrics for success of said
10 actions.

11 (D) Disrupting ransomware criminal ac-
12 tors, associated infrastructure, and their fi-
13 nances.

14 (E) Facilitating coordination and collabo-
15 ration between Federal entities and relevant en-
16 tities, including the private sector, to improve
17 Federal actions against ransomware threats.

18 (F) Collection, sharing, and analysis of
19 ransomware trends to inform Federal actions.

20 (G) Creation of after-action reports and
21 other lessons learned from Federal actions that
22 identify successes and failures to improve sub-
23 sequent actions.

1 (H) Any other activities determined appro-
2 priate by the Joint Ransomware Task Force to
3 mitigate the threat of ransomware attacks.

4 (b) RULE OF CONSTRUCTION.—Nothing in this sec-
5 tion shall be construed to provide any additional authority
6 to any Federal agency.

7 **SEC. 207. CONGRESSIONAL REPORTING.**

8 (a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not
9 later than 30 days after the date on which the Director
10 issues the final rule under section 2242(b) of the Home-
11 land Security Act of 2002, as added by section 203(b) of
12 this title, the Director shall submit to the Committee on
13 Homeland Security and Governmental Affairs of the Sen-
14 ate and the Committee on Homeland Security of the
15 House of Representatives a report that describes how the
16 Director engaged stakeholders in the development of the
17 final rule.

18 (b) REPORT ON OPPORTUNITIES TO STRENGTHEN
19 SECURITY RESEARCH.—Not later than 1 year after the
20 date of enactment of this Act, the Director shall submit
21 to the Committee on Homeland Security and Govern-
22 mental Affairs of the Senate and the Committee on Home-
23 land Security of the House of Representatives a report de-
24 scribing how the National Cybersecurity and Communica-
25 tions Integration Center established under section 2209

1 of the Homeland Security Act of 2002 (6 U.S.C. 659) has
2 carried out activities under section 2241(a)(9) of the
3 Homeland Security Act of 2002, as added by section
4 203(a) of this title, by proactively identifying opportunities
5 to use cyber incident data to inform and enable cybersecu-
6 rity research within the academic and private sector.

7 (c) REPORT ON RANSOMWARE VULNERABILITY
8 WARNING PILOT PROGRAM.—Not later than 1 year after
9 the date of enactment of this Act, and annually thereafter
10 for the duration of the pilot program established under
11 section 205, the Director shall submit to the Committee
12 on Homeland Security and Governmental Affairs of the
13 Senate and the Committee on Homeland Security of the
14 House of Representatives a report, which may include a
15 classified annex, on the effectiveness of the pilot program,
16 which shall include a discussion of the following:

17 (1) The effectiveness of the notifications under
18 section 205(c) in mitigating security vulnerabilities
19 and the threat of ransomware.

20 (2) Identification of the most common
21 vulnerabilities utilized in ransomware.

22 (3) The number of notifications issued during
23 the preceding year.

24 (4) To the extent practicable, the number of
25 vulnerable devices or systems mitigated under the

1 pilot program by the Agency during the preceding
2 year.

3 (d) REPORT ON HARMONIZATION OF REPORTING
4 REGULATIONS.—

5 (1) IN GENERAL.—Not later than 180 days
6 after the date on which the Secretary of Homeland
7 Security convenes the Cyber Incident Reporting
8 Council described in section 2246 of the Homeland
9 Security Act of 2002, as added by section 203 of
10 this title, the Secretary of Homeland Security shall
11 submit to the appropriate congressional committees
12 a report that includes—

13 (A) a list of duplicative Federal cyber inci-
14 dent reporting requirements on covered entities;

15 (B) a description of any challenges in har-
16 monizing the duplicative reporting require-
17 ments;

18 (C) any actions the Director intends to
19 take to facilitate harmonizing the duplicative
20 reporting requirements; and

21 (D) any proposed legislative changes nec-
22 essary to address the duplicative reporting.

23 (2) RULE OF CONSTRUCTION.—Nothing in
24 paragraph (1) shall be construed to provide any ad-
25 ditional regulatory authority to any Federal agency.

1 (e) GAO REPORTS.—

2 (1) IMPLEMENTATION OF THIS ACT.—Not later
3 than 2 years after the date of enactment of this Act,
4 the Comptroller General of the United States shall
5 submit to the Committee on Homeland Security and
6 Governmental Affairs of the Senate and the Com-
7 mittee on Homeland Security of the House of Rep-
8 resentatives a report on the implementation of this
9 Act and the amendments made by this Act.

10 (2) EXEMPTIONS TO REPORTING.—Not later
11 than 1 year after the date on which the Director
12 issues the final rule required under section 2242(b)
13 of the Homeland Security Act of 2002, as added by
14 section 203 of this title, the Comptroller General of
15 the United States shall submit to the Committee on
16 Homeland Security and Governmental Affairs of the
17 Senate and the Committee on Homeland Security of
18 the House of Representatives a report on the exemp-
19 tions to reporting under paragraphs (2) and (5) of
20 section 2242(a) of the Homeland Security Act of
21 2002, as added by section 203 of this title, which
22 shall include—

23 (A) to the extent practicable, an evaluation
24 of the quantity of cyber incidents not reported
25 to the Federal Government;

1 (B) an evaluation of the impact on im-
2 pacted entities, homeland security, and the na-
3 tional economy due to cyber incidents,
4 ransomware attacks, and ransom payments, in-
5 cluding a discussion on the scope of impact of
6 cyber incidents that were not reported to the
7 Federal Government;

8 (C) an evaluation of the burden, financial
9 and otherwise, on entities required to report
10 cyber incidents under this Act, including an
11 analysis of entities that meet the definition of
12 a small business concern under section 3 of the
13 Small Business Act (15 U.S.C. 632); and

14 (D) a description of the consequences and
15 effects of limiting covered cyber incident and
16 ransom payment reporting to only covered enti-
17 ties.

18 (f) REPORT ON EFFECTIVENESS OF ENFORCEMENT
19 MECHANISMS.—Not later than 1 year after the date on
20 which the Director issues the final rule required under sec-
21 tion 2242(b) of the Homeland Security Act of 2002, as
22 added by section 203 of this title, the Director shall sub-
23 mit to the Committee on Homeland Security and Govern-
24 mental Affairs of the Senate and the Committee on Home-
25 land Security of the House of Representatives a report on

1 the effectiveness of the enforcement mechanisms within
2 section 2244 of the Homeland Security Act of 2002, as
3 added by section 203 of this title.

4 **TITLE III—FEDERAL SECURE**
5 **CLOUD IMPROVEMENT AND**
6 **JOBS ACT OF 2022**

7 **SEC. 301. SHORT TITLE.**

8 This title may be cited as the “Federal Secure Cloud
9 Improvement and Jobs Act of 2022”.

10 **SEC. 302. FINDINGS.**

11 Congress finds the following:

12 (1) Ensuring that the Federal Government can
13 securely leverage cloud computing products and serv-
14 ices is key to expediting the modernization of legacy
15 information technology systems, increasing cyberse-
16 curity within and across departments and agencies,
17 and supporting the continued leadership of the
18 United States in technology innovation and job cre-
19 ation.

20 (2) According to independent analysis, as of
21 calendar year 2019, the size of the cloud computing
22 market had tripled since 2004, enabling more than
23 2,000,000 jobs and adding more than
24 \$200,000,000,000 to the gross domestic product of
25 the United States.

1 (3) The Federal Government, across multiple
2 presidential administrations and Congresses, has
3 continued to support the ability of agencies to move
4 to the cloud, including through—

5 (A) President Barack Obama’s “Cloud
6 First Strategy”;

7 (B) President Donald Trump’s “Cloud
8 Smart Strategy”;

9 (C) the prioritization of cloud security in
10 Executive Order 14028 (86 Fed. Reg. 26633;
11 relating to improving the nation’s cybersecu-
12 rity), which was issued by President Joe Biden;
13 and

14 (D) more than a decade of appropriations
15 and authorization legislation that provides
16 agencies with relevant authorities and appro-
17 priations to modernize on-premises information
18 technology systems and more readily adopt
19 cloud computing products and services.

20 (4) Since it was created in 2011, the Federal
21 Risk and Authorization Management Program (re-
22 ferred to in this section as “FedRAMP”) at the
23 General Services Administration has made steady
24 and sustained improvements in supporting the se-
25 cure authorization and reuse of cloud computing

1 products and services within the Federal Govern-
2 ment, including by reducing the costs and burdens
3 on both agencies and cloud companies to quickly and
4 securely enter the Federal market.

5 (5) According to data from the General Services
6 Administration, as of the end of fiscal year 2021,
7 there were 239 cloud providers with FedRAMP au-
8 thorizations, and those authorizations had been re-
9 used more than 2,700 times across various agencies.

10 (6) Providing a legislative framework for
11 FedRAMP and new authorities to the General Serv-
12 ices Administration, the Office of Management and
13 Budget, and Federal agencies will—

14 (A) improve the speed at which new cloud
15 computing products and services can be se-
16 curely authorized;

17 (B) enhance the ability of agencies to ef-
18 fectively evaluate FedRAMP authorized pro-
19 viders for reuse;

20 (C) reduce the costs and burdens to cloud
21 providers seeking a FedRAMP authorization;
22 and

23 (D) provide for more robust transparency
24 and dialogue between industry and the Federal
25 Government to drive stronger adoption of se-

1 cure cloud capabilities, create jobs, and reduce
2 wasteful legacy information technology.

3 **SEC. 303. TITLE 44 AMENDMENTS.**

4 (a) AMENDMENT.—Chapter 36 of title 44, United
5 States Code, is amended by adding at the end the fol-
6 lowing:

7 **“§ 3607. Definitions**

8 “(a) IN GENERAL.—Except as provided under sub-
9 section (b), the definitions under sections 3502 and 3552
10 apply to this section through section 3616.

11 “(b) ADDITIONAL DEFINITIONS.—In this section
12 through section 3616:

13 “(1) ADMINISTRATOR.—The term ‘Adminis-
14 trator’ means the Administrator of General Services.

15 “(2) APPROPRIATE CONGRESSIONAL COMMIT-
16 TEES.—The term ‘appropriate congressional com-
17 mittees’ means the Committee on Homeland Secu-
18 rity and Governmental Affairs of the Senate and the
19 Committee on Oversight and Reform of the House
20 of Representatives.

21 “(3) AUTHORIZATION TO OPERATE; FEDERAL
22 INFORMATION.—The terms ‘authorization to oper-
23 ate’ and ‘Federal information’ have the meaning
24 given those term in Circular A–130 of the Office of
25 Management and Budget entitled ‘Managing Infor-

1 mation as a Strategic Resource’, or any successor
2 document.

3 “(4) CLOUD COMPUTING.—The term ‘cloud
4 computing’ has the meaning given the term in Spe-
5 cial Publication 800–145 of the National Institute of
6 Standards and Technology, or any successor docu-
7 ment.

8 “(5) CLOUD SERVICE PROVIDER.—The term
9 ‘cloud service provider’ means an entity offering
10 cloud computing products or services to agencies.

11 “(6) FEDRAMP.—The term ‘FedRAMP’
12 means the Federal Risk and Authorization Manage-
13 ment Program established under section 3608.

14 “(7) FEDRAMP AUTHORIZATION.—The term
15 ‘FedRAMP authorization’ means a certification that
16 a cloud computing product or service has—

17 “(A) completed a FedRAMP authorization
18 process, as determined by the Administrator; or

19 “(B) received a FedRAMP provisional au-
20 thorization to operate, as determined by the
21 FedRAMP Board.

22 “(8) FEDRAMP AUTHORIZATION PACKAGE.—
23 The term ‘FedRAMP authorization package’ means
24 the essential information that can be used by an
25 agency to determine whether to authorize the oper-

1 ation of an information system or the use of a des-
 2 ignated set of common controls for all cloud com-
 3 puting products and services authorized by
 4 FedRAMP.

5 “(9) FEDRAMP BOARD.—The term ‘FedRAMP
 6 Board’ means the board established under section
 7 3610.

8 “(10) INDEPENDENT ASSESSMENT SERVICE.—
 9 The term ‘independent assessment service’ means a
 10 third-party organization accredited by the Adminis-
 11 trator to undertake conformity assessments of cloud
 12 service providers and the products or services of
 13 cloud service providers.

14 “(11) SECRETARY.—The term ‘Secretary’
 15 means the Secretary of Homeland Security.

16 **“§ 3608. Federal Risk and Authorization Management**
 17 **Program**

18 “‘There is established within the General Services Ad-
 19 ministration the Federal Risk and Authorization Manage-
 20 ment Program. The Administrator, subject to section
 21 3614, shall establish a Government-wide program that
 22 provides a standardized, reusable approach to security as-
 23 sessment and authorization for cloud computing products
 24 and services that process unclassified information used by
 25 agencies.

1 **“§ 3609. Roles and responsibilities of the General**
2 **Services Administration**

3 “(a) ROLES AND RESPONSIBILITIES.—The Adminis-
4 trator shall—

5 “(1) in consultation with the Secretary, develop,
6 coordinate, and implement a process to support
7 agency review, reuse, and standardization, where ap-
8 propriate, of security assessments of cloud com-
9 puting products and services, including, as appro-
10 priate, oversight of continuous monitoring of cloud
11 computing products and services, pursuant to guid-
12 ance issued by the Director pursuant to section
13 3614;

14 “(2) establish processes and identify criteria
15 consistent with guidance issued by the Director
16 under section 3614 to make a cloud computing prod-
17 uct or service eligible for a FedRAMP authorization
18 and validate whether a cloud computing product or
19 service has a FedRAMP authorization;

20 “(3) develop and publish templates, best prac-
21 tices, technical assistance, and other materials to
22 support the authorization of cloud computing prod-
23 ucts and services and increase the speed, effective-
24 ness, and transparency of the authorization process,
25 consistent with standards and guidelines established

1 by the Director of the National Institute of Stand-
2 ards and Technology and relevant statutes;

3 “(4) establish and update guidance on the
4 boundaries of FedRAMP authorization packages to
5 enhance the security and protection of Federal infor-
6 mation and promote transparency for agencies and
7 users as to which services are included in the scope
8 of a FedRAMP authorization;

9 “(5) grant FedRAMP authorizations to cloud
10 computing products and services consistent with the
11 guidance and direction of the FedRAMP Board;

12 “(6) establish and maintain a public comment
13 process for proposed guidance and other FedRAMP
14 directives that may have a direct impact on cloud
15 service providers and agencies before the issuance of
16 such guidance or other FedRAMP directives;

17 “(7) coordinate with the FedRAMP Board, the
18 Director of the Cybersecurity and Infrastructure Se-
19 curity Agency, and other entities identified by the
20 Administrator, with the concurrence of the Director
21 and the Secretary, to establish and regularly update
22 a framework for continuous monitoring under sec-
23 tion 3553;

24 “(8) provide a secure mechanism for storing
25 and sharing necessary data, including FedRAMP

1 authorization packages, to enable better reuse of
2 such packages across agencies, including making
3 available any information and data necessary for
4 agencies to fulfill the requirements of section 3613;

5 “(9) provide regular updates to applicant cloud
6 service providers on the status of any cloud com-
7 puting product or service during an assessment
8 process;

9 “(10) regularly review, in consultation with the
10 FedRAMP Board—

11 “(A) the costs associated with the inde-
12 pendent assessment services described in section
13 3611; and

14 “(B) the information relating to foreign in-
15 terests submitted pursuant to section 3612;

16 “(11) in coordination with the Director of the
17 National Institute of Standards and Technology, the
18 Director, the Secretary, and other stakeholders, as
19 appropriate, determine the sufficiency of underlying
20 standards and requirements to identify and assess
21 the provenance of the software in cloud services and
22 products;

23 “(12) support the Federal Secure Cloud Advi-
24 sory Committee established pursuant to section
25 3616; and

1 “(13) take such other actions as the Adminis-
2 trator may determine necessary to carry out
3 FedRAMP.

4 “(b) WEBSITE.—

5 “(1) IN GENERAL.—The Administrator shall
6 maintain a public website to serve as the authori-
7 tative repository for FedRAMP, including the timely
8 publication and updates for all relevant information,
9 guidance, determinations, and other materials re-
10 quired under subsection (a).

11 “(2) CRITERIA AND PROCESS FOR FEDRAMP
12 AUTHORIZATION PRIORITIES.—The Administrator
13 shall develop and make publicly available on the
14 website described in paragraph (1) the criteria and
15 process for prioritizing and selecting cloud com-
16 puting products and services that will receive a
17 FedRAMP authorization, in consultation with the
18 FedRAMP Board and the Chief Information Offi-
19 cers Council.

20 “(c) EVALUATION OF AUTOMATION PROCEDURES.—

21 “(1) IN GENERAL.—The Administrator, in co-
22 ordination with the Secretary, shall assess and
23 evaluate available automation capabilities and proce-
24 dures to improve the efficiency and effectiveness of
25 the issuance of FedRAMP authorizations, including

1 continuous monitoring of cloud computing products
2 and services.

3 “(2) MEANS FOR AUTOMATION.—Not later than
4 1 year after the date of enactment of this section,
5 and updated regularly thereafter, the Administrator
6 shall establish a means for the automation of secu-
7 rity assessments and reviews.

8 “(d) METRICS FOR AUTHORIZATION.—The Adminis-
9 trator shall establish annual metrics regarding the time
10 and quality of the assessments necessary for completion
11 of a FedRAMP authorization process in a manner that
12 can be consistently tracked over time in conjunction with
13 the periodic testing and evaluation process pursuant to
14 section 3554 in a manner that minimizes the agency re-
15 porting burden.

16 **“§ 3610. FedRAMP Board**

17 “(a) ESTABLISHMENT.—There is established a
18 FedRAMP Board to provide input and recommendations
19 to the Administrator regarding the requirements and
20 guidelines for, and the prioritization of, security assess-
21 ments of cloud computing products and services.

22 “(b) MEMBERSHIP.—The FedRAMP Board shall
23 consist of not more than 7 senior officials or experts from
24 agencies appointed by the Director, in consultation with
25 the Administrator, from each of the following:

1 “(1) The Department of Defense.

2 “(2) The Department of Homeland Security.

3 “(3) The General Services Administration.

4 “(4) Such other agencies as determined by the
5 Director, in consultation with the Administrator.

6 “(c) QUALIFICATIONS.—Members of the FedRAMP
7 Board appointed under subsection (b) shall have technical
8 expertise in domains relevant to FedRAMP, such as—

9 “(1) cloud computing;

10 “(2) cybersecurity;

11 “(3) privacy;

12 “(4) risk management; and

13 “(5) other competencies identified by the Direc-
14 tor to support the secure authorization of cloud serv-
15 ices and products.

16 “(d) DUTIES.—The FedRAMP Board shall—

17 “(1) in consultation with the Administrator,
18 serve as a resource for best practices to accelerate
19 the process for obtaining a FedRAMP authorization;

20 “(2) establish and regularly update require-
21 ments and guidelines for security authorizations of
22 cloud computing products and services, consistent
23 with standards and guidelines established by the Di-
24 rector of the National Institute of Standards and

1 Technology, to be used in the determination of
2 FedRAMP authorizations;

3 “(3) monitor and oversee, to the greatest extent
4 practicable, the processes and procedures by which
5 agencies determine and validate requirements for a
6 FedRAMP authorization, including periodic review
7 of the agency determinations described in section
8 3613(b);

9 “(4) ensure consistency and transparency be-
10 tween agencies and cloud service providers in a man-
11 ner that minimizes confusion and engenders trust;
12 and

13 “(5) perform such other roles and responsibil-
14 ities as the Director may assign, with concurrence
15 from the Administrator.

16 “(e) DETERMINATIONS OF DEMAND FOR CLOUD
17 COMPUTING PRODUCTS AND SERVICES.—The FedRAMP
18 Board may consult with the Chief Information Officers
19 Council to establish a process, which may be made avail-
20 able on the website maintained under section 3609(b), for
21 prioritizing and accepting the cloud computing products
22 and services to be granted a FedRAMP authorization.

23 **“§ 3611. Independent assessment**

24 “The Administrator may determine whether
25 FedRAMP may use an independent assessment service to

1 analyze, validate, and attest to the quality and compliance
 2 of security assessment materials provided by cloud service
 3 providers during the course of a determination of whether
 4 to use a cloud computing product or service.

5 **“§ 3612. Declaration of foreign interests**

6 “(a) IN GENERAL.—An independent assessment serv-
 7 ice that performs services described in section 3611 shall
 8 annually submit to the Administrator information relating
 9 to any foreign interest, foreign influence, or foreign con-
 10 trol of the independent assessment service.

11 “(b) UPDATES.—Not later than 48 hours after there
 12 is a change in foreign ownership or control of an inde-
 13 pendent assessment service that performs services de-
 14 scribed in section 3611, the independent assessment serv-
 15 ice shall submit to the Administrator an update to the in-
 16 formation submitted under subsection (a).

17 “(c) CERTIFICATION.—The Administrator may re-
 18 quire a representative of an independent assessment serv-
 19 ice to certify the accuracy and completeness of any infor-
 20 mation submitted under this section.

21 **“§ 3613. Roles and responsibilities of agencies**

22 “(a) IN GENERAL.—In implementing the require-
 23 ments of FedRAMP, the head of each agency shall, con-
 24 sistent with guidance issued by the Director pursuant to
 25 section 3614—

1 “(1) promote the use of cloud computing prod-
2 ucts and services that meet FedRAMP security re-
3 quirements and other risk-based performance re-
4 quirements as determined by the Director, in con-
5 sultation with the Secretary;

6 “(2) confirm whether there is a FedRAMP au-
7 thorization in the secure mechanism provided under
8 section 3609(a)(8) before beginning the process of
9 granting a FedRAMP authorization for a cloud com-
10 puting product or service;

11 “(3) to the extent practicable, for any cloud
12 computing product or service the agency seeks to au-
13 thorize that has received a FedRAMP authorization,
14 use the existing assessments of security controls and
15 materials within any FedRAMP authorization pack-
16 age for that cloud computing product or service; and

17 “(4) provide to the Director data and informa-
18 tion required by the Director pursuant to section
19 3614 to determine how agencies are meeting metrics
20 established by the Administrator.

21 “(b) ATTESTATION.—Upon completing an assess-
22 ment or authorization activity with respect to a particular
23 cloud computing product or service, if an agency deter-
24 mines that the information and data the agency has re-
25 viewed under paragraph (2) or (3) of subsection (a) is

1 wholly or substantially deficient for the purposes of per-
2 forming an authorization of the cloud computing product
3 or service, the head of the agency shall document as part
4 of the resulting FedRAMP authorization package the rea-
5 sons for this determination.

6 “(c) SUBMISSION OF AUTHORIZATIONS TO OPERATE
7 REQUIRED.—Upon issuance of an agency authorization to
8 operate based on a FedRAMP authorization, the head of
9 the agency shall provide a copy of its authorization to op-
10 erate letter and any supplementary information required
11 pursuant to section 3609(a) to the Administrator.

12 “(d) SUBMISSION OF POLICIES REQUIRED.—Not
13 later than 180 days after the date on which the Director
14 issues guidance in accordance with section 3614(1), the
15 head of each agency, acting through the chief information
16 officer of the agency, shall submit to the Director all agen-
17 cy policies relating to the authorization of cloud computing
18 products and services.

19 “(e) PRESUMPTION OF ADEQUACY.—

20 “(1) IN GENERAL.—The assessment of security
21 controls and materials within the authorization
22 package for a FedRAMP authorization shall be pre-
23 sumed adequate for use in an agency authorization
24 to operate cloud computing products and services.

1 “(2) INFORMATION SECURITY REQUIRE-
2 MENTS.—The presumption under paragraph (1)
3 does not modify or alter—

4 “(A) the responsibility of any agency to en-
5 sure compliance with subchapter II of chapter
6 35 for any cloud computing product or service
7 used by the agency; or

8 “(B) the authority of the head of any
9 agency to make a determination that there is a
10 demonstrable need for additional security re-
11 quirements beyond the security requirements
12 included in a FedRAMP authorization for a
13 particular control implementation.

14 **“§ 3614. Roles and responsibilities of the Office of**
15 **Management and Budget**

16 “The Director shall—

17 “(1) in consultation with the Administrator and
18 the Secretary, issue guidance that—

19 “(A) specifies the categories or characteris-
20 tics of cloud computing products and services
21 that are within the scope of FedRAMP;

22 “(B) includes requirements for agencies to
23 obtain a FedRAMP authorization when oper-
24 ating a cloud computing product or service de-

1 scribed in subparagraph (A) as a Federal infor-
2 mation system; and

3 “(C) encompasses, to the greatest extent
4 practicable, all necessary and appropriate cloud
5 computing products and services;

6 “(2) issue guidance describing additional re-
7 sponsibilities of FedRAMP and the FedRAMP
8 Board to accelerate the adoption of secure cloud
9 computing products and services by the Federal
10 Government;

11 “(3) in consultation with the Administrator, es-
12 tablish a process to periodically review FedRAMP
13 authorization packages to support the secure author-
14 ization and reuse of secure cloud products and serv-
15 ices;

16 “(4) oversee the effectiveness of FedRAMP and
17 the FedRAMP Board, including the compliance by
18 the FedRAMP Board with the duties described in
19 section 3610(d); and

20 “(5) to the greatest extent practicable, encour-
21 age and promote consistency of the assessment, au-
22 thorization, adoption, and use of secure cloud com-
23 puting products and services within and across agen-
24 cies.

1 **“§ 3615. Reports to Congress; GAO report**

2 “(a) REPORTS TO CONGRESS.—Not later than 1 year
3 after the date of enactment of this section, and annually
4 thereafter, the Director shall submit to the appropriate
5 congressional committees a report that includes the fol-
6 lowing:

7 “(1) During the preceding year, the status, effi-
8 ciency, and effectiveness of the General Services Ad-
9 ministration under section 3609 and agencies under
10 section 3613 and in supporting the speed, effective-
11 ness, sharing, reuse, and security of authorizations
12 to operate for secure cloud computing products and
13 services.

14 “(2) Progress towards meeting the metrics re-
15 quired under section 3609(d).

16 “(3) Data on FedRAMP authorizations.

17 “(4) The average length of time to issue
18 FedRAMP authorizations.

19 “(5) The number of FedRAMP authorizations
20 submitted, issued, and denied for the preceding year.

21 “(6) A review of progress made during the pre-
22 ceding year in advancing automation techniques to
23 securely automate FedRAMP processes and to accel-
24 erate reporting under this section.

25 “(7) The number and characteristics of author-
26 ized cloud computing products and services in use at

1 each agency consistent with guidance provided by
2 the Director under section 3614.

3 “(8) A review of FedRAMP measures to ensure
4 the security of data stored or processed by cloud
5 service providers, which may include—

6 “(A) geolocation restrictions for provided
7 products or services;

8 “(B) disclosures of foreign elements of
9 supply chains of acquired products or services;

10 “(C) continued disclosures of ownership of
11 cloud service providers by foreign entities; and

12 “(D) encryption for data processed, stored,
13 or transmitted by cloud service providers.

14 “(b) GAO REPORT.—Not later than 180 days after
15 the date of enactment of this section, the Comptroller
16 General of the United States shall report to the appro-
17 priate congressional committees an assessment of the fol-
18 lowing:

19 “(1) The costs incurred by agencies and cloud
20 service providers relating to the issuance of
21 FedRAMP authorizations.

22 “(2) The extent to which agencies have proc-
23 esses in place to continuously monitor the implemen-
24 tation of cloud computing products and services op-
25 erating as Federal information systems.

1 “(3) How often and for which categories of
2 products and services agencies use FedRAMP au-
3 thorizations.

4 “(4) The unique costs and potential burdens in-
5 curred by cloud computing companies that are small
6 business concerns (as defined in section 3(a) of the
7 Small Business Act (15 U.S.C. 632(a)) as a part of
8 the FedRAMP authorization process.

9 **“§ 3616. Federal Secure Cloud Advisory Committee**

10 “(a) ESTABLISHMENT, PURPOSES, AND DUTIES.—

11 “(1) ESTABLISHMENT.—There is established a
12 Federal Secure Cloud Advisory Committee (referred
13 to in this section as the ‘Committee’) to ensure ef-
14 fective and ongoing coordination of agency adoption,
15 use, authorization, monitoring, acquisition, and secu-
16 rity of cloud computing products and services to en-
17 able agency mission and administrative priorities.

18 “(2) PURPOSES.—The purposes of the Com-
19 mittee are the following:

20 “(A) To examine the operations of
21 FedRAMP and determine ways that authoriza-
22 tion processes can continuously be improved, in-
23 cluding the following:

24 “(i) Measures to increase agency
25 reuse of FedRAMP authorizations.

1 “(ii) Proposed actions that can be
2 adopted to reduce the burden, confusion,
3 and cost associated with FedRAMP au-
4 thorizations for cloud service providers.

5 “(iii) Measures to increase the num-
6 ber of FedRAMP authorizations for cloud
7 computing products and services offered by
8 small businesses concerns (as defined by
9 section 3(a) of the Small Business Act (15
10 U.S.C. 632(a)).

11 “(iv) Proposed actions that can be
12 adopted to reduce the burden and cost of
13 FedRAMP authorizations for agencies.

14 “(B) Collect information and feedback on
15 agency compliance with and implementation of
16 FedRAMP requirements.

17 “(C) Serve as a forum that facilitates com-
18 munication and collaboration among the
19 FedRAMP stakeholder community.

20 “(3) DUTIES.—The duties of the Committee in-
21 clude providing advice and recommendations to the
22 Administrator, the FedRAMP Board, and agencies
23 on technical, financial, programmatic, and oper-
24 ational matters regarding secure adoption of cloud
25 computing products and services.

1 “(b) MEMBERS.—

2 “(1) COMPOSITION.—The Committee shall be
3 comprised of not more than 15 members who are
4 qualified representatives from the public and private
5 sectors, appointed by the Administrator, in consulta-
6 tion with the Director, as follows:

7 “(A) The Administrator or the Administra-
8 tor’s designee, who shall be the Chair of the
9 Committee.

10 “(B) At least 1 representative each from
11 the Cybersecurity and Infrastructure Security
12 Agency and the National Institute of Standards
13 and Technology.

14 “(C) At least 2 officials who serve as the
15 Chief Information Security Officer within an
16 agency, who shall be required to maintain such
17 a position throughout the duration of their serv-
18 ice on the Committee.

19 “(D) At least 1 official serving as Chief
20 Procurement Officer (or equivalent) in an agen-
21 cy, who shall be required to maintain such a po-
22 sition throughout the duration of their service
23 on the Committee.

24 “(E) At least 1 individual representing an
25 independent assessment service.

1 “(F) At least 5 representatives from
2 unique businesses that primarily provide cloud
3 computing services or products, including at
4 least 2 representatives from a small business
5 concern (as defined by section 3(a) of the Small
6 Business Act (15 U.S.C. 632(a))).

7 “(G) At least 2 other representatives of the
8 Federal Government as the Administrator de-
9 termines necessary to provide sufficient balance,
10 insights, or expertise to the Committee.

11 “(2) DEADLINE FOR APPOINTMENT.—Each
12 member of the Committee shall be appointed not
13 later than 90 days after the date of enactment of
14 this section.

15 “(3) PERIOD OF APPOINTMENT; VACANCIES.—

16 “(A) IN GENERAL.—Each non-Federal
17 member of the Committee shall be appointed
18 for a term of 3 years, except that the initial
19 terms for members may be staggered 1-, 2-, or
20 3-year terms to establish a rotation in which
21 one-third of the members are selected each
22 year. Any such member may be appointed for
23 not more than 2 consecutive terms.

24 “(B) VACANCIES.—Any vacancy in the
25 Committee shall not affect its powers, but shall

1 be filled in the same manner in which the origi-
2 nal appointment was made. Any member ap-
3 pointed to fill a vacancy occurring before the
4 expiration of the term for which the member's
5 predecessor was appointed shall be appointed
6 only for the remainder of that term. A member
7 may serve after the expiration of that member's
8 term until a successor has taken office.

9 “(c) MEETINGS AND RULES OF PROCEDURES.—

10 “(1) MEETINGS.—The Committee shall hold
11 not fewer than 3 meetings in a calendar year, at
12 such time and place as determined by the Chair.

13 “(2) INITIAL MEETING.—Not later than 120
14 days after the date of enactment of this section, the
15 Committee shall meet and begin the operations of
16 the Committee.

17 “(3) RULES OF PROCEDURE.—The Committee
18 may establish rules for the conduct of the business
19 of the Committee if such rules are not inconsistent
20 with this section or other applicable law.

21 “(d) EMPLOYEE STATUS.—

22 “(1) IN GENERAL.—A member of the Com-
23 mittee (other than a member who is appointed to the
24 Committee in connection with another Federal ap-
25 pointment) shall not be considered an employee of

1 the Federal Government by reason of any service as
2 such a member, except for the purposes of section
3 5703 of title 5, relating to travel expenses.

4 “(2) PAY NOT PERMITTED.—A member of the
5 Committee covered by paragraph (1) may not receive
6 pay by reason of service on the Committee.

7 “(e) APPLICABILITY TO THE FEDERAL ADVISORY
8 COMMITTEE ACT.—Section 14 of the Federal Advisory
9 Committee Act (5 U.S.C. App.) shall not apply to the
10 Committee.

11 “(f) DETAIL OF EMPLOYEES.—Any Federal Govern-
12 ment employee may be detailed to the Committee without
13 reimbursement from the Committee, and such detailee
14 shall retain the rights, status, and privileges of his or her
15 regular employment without interruption.

16 “(g) POSTAL SERVICES.—The Committee may use
17 the United States mails in the same manner and under
18 the same conditions as agencies.

19 “(h) REPORTS.—

20 “(1) INTERIM REPORTS.—The Committee may
21 submit to the Administrator and Congress interim
22 reports containing such findings, conclusions, and
23 recommendations as have been agreed to by the
24 Committee.

1 “(2) ANNUAL REPORTS.—Not later than 540
 2 days after the date of enactment of this section, and
 3 annually thereafter, the Committee shall submit to
 4 the Administrator and Congress a report containing
 5 such findings, conclusions, and recommendations as
 6 have been agreed to by the Committee.”.

7 (b) TECHNICAL AND CONFORMING AMENDMENT.—
 8 The table of sections for chapter 36 of title 44, United
 9 States Code, is amended by adding at the end the fol-
 10 lowing new items:

“3607. Definitions.

“3608. Federal Risk and Authorization Management Program.

“3609. Roles and responsibilities of the General Services Administration.

“3610. FedRAMP Board.

“3611. Independent assessment.

“3612. Declaration of foreign interests.

“3613. Roles and responsibilities of agencies.

“3614. Roles and responsibilities of the Office of Management and Budget.

“3615. Reports to Congress; GAO report.

“3616. Federal Secure Cloud Advisory Committee.”.

11 (c) SUNSET.—

12 (1) IN GENERAL.—Effective on the date that is
 13 5 years after the date of enactment of this Act,
 14 chapter 36 of title 44, United States Code, is
 15 amended by striking sections 3607 through 3616.

16 (2) CONFORMING AMENDMENT.—Effective on
 17 the date that is 5 years after the date of enactment
 18 of this Act, the table of sections for chapter 36 of
 19 title 44, United States Code, is amended by striking
 20 the items relating to sections 3607 through 3616.

1 (d) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion or any amendment made by this section shall be con-
3 strued as altering or impairing the authorities of the Di-
4 rector of the Office of Management and Budget or the
5 Secretary of Homeland Security under subchapter II of
6 chapter 35 of title 44, United States Code.

Calendar No. 265

117TH CONGRESS
2^D Session

S. 3600

A BILL

To improve the cybersecurity of the Federal
Government, and for other purposes.

FEBRUARY 9, 2022

Read the second time and placed on the calendar