

118TH CONGRESS
1ST SESSION

H. R. 4552

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

IN THE HOUSE OF REPRESENTATIVES

JULY 11, 2023

Ms. MACE (for herself, Mr. RASKIN, Mr. COMER, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Oversight and Accountability, and in addition to the Committees on Science, Space, and Technology, Homeland Security, and Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Federal Information Security Modernization Act of
6 2023”.

7 (b) TABLE OF CONTENTS.—The table of contents for
8 this Act is as follows:

- Sec. 1. Short title; table of contents.
 Sec. 2. Definitions.
 Sec. 3. Amendments to title 44.
 Sec. 4. Amendments to subtitle III of title 40.
 Sec. 5. Actions to enhance Federal incident transparency.
 Sec. 6. Additional guidance to agencies on FISMA updates.
 Sec. 7. Agency requirements to notify private sector entities impacted by incidents.
 Sec. 8. Mobile security briefings.
 Sec. 9. Data and logging retention for incident response.
 Sec. 10. CISA agency liaisons.
 Sec. 11. Federal penetration testing policy.
 Sec. 12. Vulnerability disclosure policies.
 Sec. 13. Implementing zero trust architecture.
 Sec. 14. Automation and artificial intelligence.
 Sec. 15. Extension of chief data officer council.
 Sec. 16. Council of the Inspectors General on Integrity and Efficiency dashboard.
 Sec. 17. Security operations center shared service.
 Sec. 18. Federal cybersecurity requirements.
 Sec. 19. Federal Chief Information Security Officer.
 Sec. 20. Renaming Office of the Federal Chief Information Officer.
 Sec. 21. Rules of construction.

1 **SEC. 2. DEFINITIONS.**

2 In this Act, unless otherwise specified:

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

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

9 (A) the Committee on Homeland Security
 10 and Governmental Affairs of the Senate;

11 (B) the Committee on Oversight and Ac-
 12 countability of the House of Representatives;
 13 and

1 (C) the Committee on Homeland Security
2 of the House of Representatives.

3 (3) AWARDEE.—The term “awardee” has the
4 meaning given the term in section 3591 of title 44,
5 United States Code, as added by this Act.

6 (4) CONTRACTOR.—The term “contractor” has
7 the meaning given the term in section 3591 of title
8 44, United States Code, as added by this Act.

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

12 (6) FEDERAL INFORMATION SYSTEM.—The
13 term “Federal information system” has the meaning
14 give the term in section 3591 of title 44, United
15 States Code, as added by this Act.

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

19 (8) NATIONAL SECURITY SYSTEM.—The term
20 “national security system” has the meaning given
21 the term in section 3552(b) of title 44, United
22 States Code.

23 (9) PENETRATION TEST.—The term “penetra-
24 tion test” has the meaning given the term in section

1 3552(b) of title 44, United States Code, as amended
2 by this Act.

3 (10) THREAT HUNTING.—The term “threat
4 hunting” means proactively and iteratively searching
5 systems for threats and vulnerabilities, including
6 threats or vulnerabilities that may evade detection
7 by automated threat detection systems.

8 (11) ZERO TRUST ARCHITECTURE.—The term
9 “zero trust architecture” has the meaning given the
10 term in Special Publication 800–207 of the National
11 Institute of Standards and Technology, or any suc-
12 cessor document.

13 **SEC. 3. AMENDMENTS TO TITLE 44.**

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

16 (1) in section 3504—

17 (A) in subsection (a)(1)(B)—

18 (i) by striking clause (v) and inserting
19 the following:

20 “(v) privacy, confidentiality, disclo-
21 sure, and sharing of information;”;

22 (ii) by redesignating clause (vi) as
23 clause (vii); and

24 (iii) by inserting after clause (v) the
25 following:

1 “(vi) in consultation with the National
2 Cyber Director, security of information;
3 and”; and

4 (B) in subsection (g)—

5 (i) by redesignating paragraph (2) as
6 paragraph (3); and

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

9 “(1) develop and oversee the implementation of
10 policies, principles, standards, and guidelines on pri-
11 vacy, confidentiality, disclosure, and sharing of in-
12 formation collected or maintained by or for agencies;

13 “(2) in consultation with the National Cyber
14 Director, oversee the implementation of policies,
15 principles, standards, and guidelines on security, of
16 information collected or maintained by or for agen-
17 cies; and”;

18 (2) in section 3505—

19 (A) by striking the first subsection des-
20 igned as subsection (c);

21 (B) in paragraph (2) of the second sub-
22 section designated as subsection (c), by insert-
23 ing “an identification of internet accessible in-
24 formation systems and” after “an inventory
25 under this subsection shall include”;

1 (C) in paragraph (3) of the second sub-
2 section designated as subsection (c)—

3 (i) in subparagraph (B)—

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

9 (II) by striking “and” at the end;

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

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

15 “(D) maintained on a continual basis
16 through the use of automation, machine-read-
17 able data, and scanning, wherever practicable.”;
18 (3) in section 3506—

19 (A) in subsection (a)(3), by inserting “In
20 carrying out these duties, the Chief Information
21 Officer shall consult, as appropriate, with the
22 Chief Data Officer in accordance with the des-
23 ignated functions under section 3520(c).” after
24 “reduction of information collection burdens on
25 the public.”;

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

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

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

6 “(j)(1) Notwithstanding paragraphs (2) and (3) of
7 subsection (a), the head of each agency shall designate a
8 Chief Privacy Officer with the necessary skills, knowledge,
9 and expertise, who shall have the authority and responsi-
10 bility to—

11 “(A) lead the privacy program of the agency;
12 and

13 “(B) carry out the privacy responsibilities of
14 the agency under this chapter, section 552a of title
15 5, and guidance issued by the Director.

16 “(2) The Chief Privacy Officer of each agency shall—

17 “(A) serve in a central leadership position with-
18 in the agency;

19 “(B) have visibility into relevant agency oper-
20 ations; and

21 “(C) be positioned highly enough within the
22 agency to regularly engage with other agency leaders
23 and officials, including the head of the agency.

24 “(3) A privacy officer of an agency established under
25 a statute enacted before the date of enactment of the Fed-

1 eral Information Security Modernization Act of 2023 may
2 carry out the responsibilities under this subsection for the
3 agency.”; and

4 (4) in section 3513—

5 (A) by redesignating subsection (c) as sub-
6 section (d); and

7 (B) by inserting after subsection (b) the
8 following:

9 “(c) Each agency providing a written plan under sub-
10 section (b) shall provide any portion of the written plan
11 addressing information security to the Secretary of Home-
12 land Security and the National Cyber Director.”.

13 (b) SUBCHAPTER II DEFINITIONS.—

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

16 (A) by redesignating paragraphs (2), (3),
17 (4), (5), (6), and (7) as paragraphs (3), (4),
18 (5), (6), (8), and (10), respectively;

19 (B) by inserting after paragraph (1) the
20 following:

21 “(2) The term ‘high value asset’ means infor-
22 mation or an information system that the head of an
23 agency, using policies, principles, standards, or
24 guidelines issued by the Director under section
25 3553(a), determines to be so critical to the agency

1 that the loss or degradation of the confidentiality,
2 integrity, or availability of such information or infor-
3 mation system would have a serious impact on the
4 ability of the agency to perform the mission of the
5 agency or conduct business.”;

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

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

11 (D) in paragraph (8)(A), as so redesign-
12 ated, by striking “used” and inserting “owned,
13 managed,”;

14 (E) by inserting after paragraph (8), as so
15 redesignated, the following:

16 “(9) The term ‘penetration test’—

17 “(A) means an authorized assessment that
18 emulates attempts to gain unauthorized access
19 to, or disrupt the operations of, an information
20 system or component of an information system;
21 and

22 “(B) includes any additional meaning
23 given the term in policies, principles, standards,
24 or guidelines issued by the Director under sec-
25 tion 3553(a).”; and

1 (F) by inserting after paragraph (10), as
2 so redesignated, the following:

3 “(11) The term ‘shared service’ means a cen-
4 tralized mission capability or consolidated business
5 function that is provided to multiple organizations
6 within an agency or to multiple agencies.

7 “(12) The term ‘zero trust architecture’ has the
8 meaning given the term in Special Publication 800–
9 207 of the National Institute of Standards and
10 Technology, or any successor document.”

11 (2) CONFORMING AMENDMENTS.—

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

17 (B) TITLE 10.—

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

22 (ii) SECTION 2223.—Section
23 2223(c)(3) of title 10, United States Code,
24 is amended by striking “section

1 3552(b)(6)” and inserting “section
2 3552(b)”.

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

7 (iv) SECTION 2339a.—Section
8 2339a(e)(5) of title 10, United States
9 Code, is amended by striking “section
10 3552(b)(6)” and inserting “section
11 3552(b)”.

12 (C) HIGH-PERFORMANCE COMPUTING ACT
13 OF 1991.—Section 207(a) of the High-Perform-
14 ance Computing Act of 1991 (15 U.S.C.
15 5527(a)) is amended by striking “section
16 3552(b)(6)(A)(i)” and inserting “section
17 3552(b)(8)(A)(i)”.

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

24 (E) NATIONAL DEFENSE AUTHORIZATION
25 ACT FOR FISCAL YEAR 2013.—Section

1 933(e)(1)(B) of the National Defense Author-
2 ization Act for Fiscal Year 2013 (10 U.S.C.
3 2224 note) is amended by striking “section
4 3542(b)(2)” and inserting “section 3552(b)”.

5 (F) IKE SKELTON NATIONAL DEFENSE AU-
6 THORIZATION ACT FOR FISCAL YEAR 2011.—The
7 Ike Skelton National Defense Authorization Act
8 for Fiscal Year 2011 (Public Law 111–383) is
9 amended—

10 (i) in section 806(e)(5) (10 U.S.C.
11 2304 note), by striking “section 3542(b)”
12 and inserting “section 3552(b)”;

13 (ii) in section 931(b)(3) (10 U.S.C.
14 2223 note), by striking “section
15 3542(b)(2)” and inserting “section
16 3552(b)”;

17 (iii) in section 932(b)(2) (10 U.S.C.
18 2224 note), by striking “section
19 3542(b)(2)” and inserting “section
20 3552(b)”.

21 (G) E-GOVERNMENT ACT OF 2002.—Sec-
22 tion 301(c)(1)(A) of the E-Government Act of
23 2002 (44 U.S.C. 3501 note) is amended by
24 striking “section 3542(b)(2)” and inserting
25 “section 3552(b)”.

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

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

8 (ii) in subsection (f)—

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

12 (II) in paragraph (5), by striking
13 “section 3532(b)(2)” and inserting
14 “section 3552(b)”.

15 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II
16 of chapter 35 of title 44, United States Code, is amend-
17 ed—

18 (1) in section 3551—

19 (A) in paragraph (4), by striking “diag-
20 nose and improve” and inserting “integrate, de-
21 liver, diagnose, and improve”;

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

24 (C) in paragraph (6), by striking the pe-
25 riod at the end and inserting a semicolon; and

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

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

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

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

14 (2) in section 3553—

15 (A) in subsection (a)—

16 (i) in paragraph (5), by striking
17 “and” at the end;

18 (ii) in paragraph (6), by striking the
19 period at the end and inserting “; and”;
20 and

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

23 “(7) promoting, in consultation with the Direc-
24 tor of the Cybersecurity and Infrastructure Security
25 Agency, the National Cyber Director, and the Direc-

1 tor of the National Institute of Standards and Tech-
2 nology—

3 “(A) the use of automation to improve
4 Federal cybersecurity and visibility with respect
5 to the implementation of Federal cybersecurity;
6 and

7 “(B) the use of presumption of com-
8 promise and least privilege principles, such as
9 zero trust architecture, to improve resiliency
10 and timely response actions to incidents on
11 Federal systems.”;

12 (B) in subsection (b)—

13 (i) in the matter preceding paragraph
14 (1), by inserting “and the National Cyber
15 Director” after “Director”;

16 (ii) in paragraph (2)(A), by inserting
17 “and reporting requirements under sub-
18 chapter IV of this chapter” after “section
19 3556”;

20 (iii) by redesignating paragraphs (8)
21 and (9) as paragraphs (10) and (11), re-
22 spectively; and

23 (iv) by inserting after paragraph (7)
24 the following:

1 “(8) expeditiously seeking opportunities to re-
2 duce costs, administrative burdens, and other bar-
3 riers to information technology security and mod-
4 ernization for agencies, including through shared
5 services for cybersecurity capabilities identified as
6 appropriate by the Director, in coordination with the
7 Director of the Cybersecurity and Infrastructure Se-
8 curity Agency and other agencies as appropriate;”;

9 (C) in subsection (c)—

10 (i) in the matter preceding paragraph

11 (1)—

12 (I) by striking “each year” and
13 inserting “each year during which
14 agencies are required to submit re-
15 ports under section 3554(c)”;

16 (II) by inserting “, which shall be
17 unclassified but may include 1 or
18 more annexes that contain classified
19 or other sensitive information, as ap-
20 propriate” after “a report”; and

21 (III) by striking “preceding
22 year” and inserting “preceding 2
23 years”;

24 (ii) by striking paragraph (1);

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

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

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

8 “(4) a summary of the risks and trends identi-
9 fied in the Federal risk assessment required under
10 subsection (i); and”;

11 (D) in subsection (h)—

12 (i) in paragraph (2)—

13 (I) in subparagraph (A), by in-
14 serting “and the National Cyber Di-
15 rector” after “in coordination with the
16 Director”; and

17 (II) in subparagraph (D), by in-
18 serting “, the National Cyber Direc-
19 tor,” after “notify the Director”; and

20 (ii) in paragraph (3)(A)(iv), by insert-
21 ing “, the National Cyber Director,” after
22 “the Secretary provides prior notice to the
23 Director”;

24 (E) by amending subsection (i) to read as
25 follows:

1 “(i) FEDERAL RISK ASSESSMENT.—On an ongoing
2 and continuous basis, the Director of the Cybersecurity
3 and Infrastructure Security Agency shall assess the Fed-
4 eral risk posture using any available information on the
5 cybersecurity posture of agencies, and brief the Director
6 and National Cyber Director on the findings of such as-
7 sessment, including—

8 “(1) the status of agency cybersecurity remedial
9 actions for high value assets described in section
10 3554(b)(7);

11 “(2) any vulnerability information relating to
12 the systems of an agency that is known by the agen-
13 cy;

14 “(3) analysis of incident information under sec-
15 tion 3597;

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

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

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

22 “(7) evaluation of Federal and non-Federal
23 cyber threat intelligence;

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

1 “(9) agency system risk assessments required
2 under section 3554(a)(1)(A);

3 “(10) relevant reports from inspectors general
4 of agencies and the Government Accountability Of-
5 fice; and

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

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

10 “(m) DIRECTIVES.—

11 “(1) EMERGENCY DIRECTIVE UPDATES.—If the
12 Secretary issues an emergency directive under this
13 section, the Director of the Cybersecurity and Infra-
14 structure Security Agency shall submit to the Direc-
15 tor, the National Cyber Director, the Committee on
16 Homeland Security and Governmental Affairs of the
17 Senate, and the Committees on Oversight and Ac-
18 countability and Homeland Security of the House of
19 Representatives an update on the status of the im-
20 plementation of the emergency directive at agencies
21 not later than 7 days after the date on which the
22 emergency directive requires an agency to complete
23 a requirement specified by the emergency directive,
24 and every 30 days thereafter until—

1 “(A) the date on which every agency has
2 fully implemented the emergency directive;

3 “(B) the Secretary determines that an
4 emergency directive no longer requires active
5 reporting from agencies or additional implemen-
6 tation; or

7 “(C) the date that is 1 year after the
8 issuance of the directive.

9 “(2) BINDING OPERATIONAL DIRECTIVE UP-
10 DATES.—If the Secretary issues a binding oper-
11 ational directive under this section, the Director of
12 the Cybersecurity and Infrastructure Security Agen-
13 cy shall submit to the Director, the National Cyber
14 Director, the Committee on Homeland Security and
15 Governmental Affairs of the Senate, and the Com-
16 mittees on Oversight and Accountability and Home-
17 land Security of the House of Representatives an
18 update on the status of the implementation of the
19 binding operational directive at agencies not later
20 than 30 days after the issuance of the binding oper-
21 ational directive, and every 90 days thereafter
22 until—

23 “(A) the date on which every agency has
24 fully implemented the binding operational direc-
25 tive;

1 “(B) the Secretary determines that a bind-
2 ing operational directive no longer requires ac-
3 tive reporting from agencies or additional im-
4 plementation; or

5 “(C) the date that is 1 year after the
6 issuance or substantive update of the directive.

7 “(3) REPORT.—If the Director of the Cyberse-
8 curity and Infrastructure Security Agency ceases
9 submitting updates required under paragraphs (1)
10 or (2) on the date described in paragraph (1)(C) or
11 (2)(C), the Director of the Cybersecurity and Infra-
12 structure Security Agency shall submit to the Direc-
13 tor, the National Cyber Director, the Committee on
14 Homeland Security and Governmental Affairs of the
15 Senate, and the Committees on Oversight and Ac-
16 countability and Homeland Security of the House of
17 Representatives a list of every agency that, at the
18 time of the report—

19 “(A) has not completed a requirement
20 specified by an emergency directive; or

21 “(B) has not implemented a binding oper-
22 ational directive.

23 “(n) REVIEW OF OFFICE OF MANAGEMENT AND
24 BUDGET GUIDANCE AND POLICY.—

1 “(1) CONDUCT OF REVIEW.—Not less fre-
2 quently than once every 3 years, the Director of the
3 Office of Management and Budget shall review the
4 efficacy of the guidance and policy promulgated by
5 the Director in reducing cybersecurity risks, includ-
6 ing a consideration of reporting and compliance bur-
7 den on agencies.

8 “(2) CONGRESSIONAL NOTIFICATION.—The Di-
9 rector of the Office of Management and Budget
10 shall notify the Committee on Homeland Security
11 and Governmental Affairs of the Senate and the
12 Committee on Oversight and Accountability of the
13 House of Representatives of changes to guidance or
14 policy resulting from the review under paragraph
15 (1).

16 “(3) GAO REVIEW.—The Government Account-
17 ability Office shall review guidance and policy pro-
18 mulgated by the Director to assess its efficacy in
19 risk reduction and burden on agencies.

20 “(o) AUTOMATED STANDARD IMPLEMENTATION
21 VERIFICATION.—When the Director of the National Insti-
22 tute of Standards and Technology issues a proposed
23 standard or guideline pursuant to paragraphs (2) or (3)
24 of section 20(a) of the National Institute of Standards and
25 Technology Act (15 U.S.C. 278g–3(a)), the Director of

1 the National Institute of Standards and Technology shall
2 consider developing and, if appropriate and practical, de-
3 velop specifications to enable the automated verification
4 of the implementation of the controls.

5 “(p) INSPECTORS GENERAL ACCESS TO FEDERAL
6 RISK ASSESSMENTS.—The Director of the Cybersecurity
7 and Infrastructure Security Agency shall, upon request,
8 make available Federal risk assessment information under
9 subsection (i) to the Inspector General of the Department
10 of Homeland Security and the inspector general of any
11 agency that was included in the Federal risk assessment.”;

12 (3) in section 3554—

13 (A) in subsection (a)—

14 (i) in paragraph (1)—

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

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

21 “(A) on an ongoing and continuous basis,
22 assessing agency system risk, as applicable,
23 by—

1 “(i) identifying and documenting the
2 high value assets of the agency using guid-
3 ance from the Director;

4 “(ii) evaluating the data assets inven-
5 toried under section 3511 for sensitivity to
6 compromises in confidentiality, integrity,
7 and availability;

8 “(iii) identifying whether the agency
9 is participating in federally offered cyber-
10 security shared services programs;

11 “(iv) identifying agency systems that
12 have access to or hold the data assets
13 inventoried under section 3511;

14 “(v) evaluating the threats facing
15 agency systems and data, including high
16 value assets, based on Federal and non-
17 Federal cyber threat intelligence products,
18 where available;

19 “(vi) evaluating the vulnerability of
20 agency systems and data, including high
21 value assets, including by analyzing—

22 “(I) the results of penetration
23 testing performed by the Department
24 of Homeland Security under section
25 3553(b)(9);

1 “(II) the results of penetration
2 testing performed under section
3 3559A;

4 “(III) information provided to
5 the agency through the vulnerability
6 disclosure program of the agency
7 under section 3559B;

8 “(IV) incidents; and

9 “(V) any other vulnerability in-
10 formation relating to agency systems
11 that is known to the agency;

12 “(vii) assessing the impacts of poten-
13 tial agency incidents to agency systems,
14 data, and operations based on the evalua-
15 tions described in clauses (ii) and (v) and
16 the agency systems identified under clause
17 (iv); and

18 “(viii) assessing the consequences of
19 potential incidents occurring on agency
20 systems that would impact systems at
21 other agencies, including due to
22 interconnectivity between different agency
23 systems or operational reliance on the op-
24 erations of the system or data in the sys-
25 tem;”;

1 (III) in subparagraph (B), as so
2 redesignated, in the matter preceding
3 clause (i), by striking “providing in-
4 formation” and inserting “using infor-
5 mation from the assessment required
6 under subparagraph (A), providing in-
7 formation”;

8 (IV) in subparagraph (C), as so
9 redesignated—

10 (aa) in clause (ii) by insert-
11 ing “binding” before “oper-
12 ational”; and

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

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

17 “(E) providing an update on the ongoing
18 and continuous assessment required under sub-
19 paragraph (A)—

20 “(i) upon request, to the inspector
21 general of the agency or the Comptroller
22 General of the United States; and

23 “(ii) at intervals determined by guid-
24 ance issued by the Director, and to the ex-

1 tent appropriate and practicable using au-
2 tomation, to—

3 “(I) the Director;

4 “(II) the Director of the Cyberse-
5 curity and Infrastructure Security
6 Agency; and

7 “(III) the National Cyber Direc-
8 tor;”;

9 (ii) in paragraph (2)—

10 (I) in subparagraph (A), by in-
11 sserting “in accordance with the agen-
12 cy system risk assessment required
13 under paragraph (1)(A)” after “infor-
14 mation systems”; and

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

21 (iii) in paragraph (3)(A)—

22 (I) in the matter preceding clause
23 (i), by striking “senior agency infor-
24 mation security officer” and inserting
25 “Chief Information Security Officer”;

1 (II) in clause (i), by striking
2 “this section” and inserting “sub-
3 sections (a) through (c)”;

4 (III) in clause (ii), by striking
5 “training and” and inserting “skills,
6 training, and”;

7 (IV) by redesignating clauses (iii)
8 and (iv) as (iv) and (v), respectively;

9 (V) by inserting after clause (ii)
10 the following:

11 “(iii) manage information security, cy-
12 bersecurity budgets, and risk and compli-
13 ance activities and explain those concepts
14 to the head of the agency and the executive
15 team of the agency;” and

16 (VI) in clause (iv), as so redesign-
17 ated, by striking “information secu-
18 rity duties as that official’s primary
19 duty” and inserting “information,
20 computer network, and technology se-
21 curity duties as the Chief Information
22 Security Officers’ primary duty”;

23 (iv) in paragraph (5), by striking “an-
24 nually” and inserting “not less frequently
25 than quarterly”; and

1 (v) in paragraph (6), by striking “offi-
2 cial delegated” and inserting “Chief Infor-
3 mation Security Officer delegated”;

4 (B) in subsection (b)—

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

7 “(1) the ongoing and continuous assessment of
8 agency system risk required under subsection
9 (a)(1)(A), which may include using guidance and
10 automated tools consistent with standards and
11 guidelines promulgated under section 11331 of title
12 40, as applicable;”;

13 (ii) in paragraph (2)—

14 (I) by striking subparagraph (B);

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

18 (III) in subparagraph (B), as so
19 redesignated, by striking “and” at the
20 end; and

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

23 (aa) by redesignating
24 clauses (iii) and (iv) as clauses
25 (iv) and (v), respectively;

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

3 “(iii) binding operational directives
4 and emergency directives issued by the
5 Secretary under section 3553;” and

6 (cc) in clause (iv), as so re-
7 designated, by striking “as deter-
8 mined by the agency; and” and
9 inserting “as determined by the
10 agency, considering the agency
11 risk assessment required under
12 subsection (a)(1)(A);

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

16 (iv) by redesignating paragraphs (7)
17 and (8) as paragraphs (8) and (9), respec-
18 tively;

19 (v) by inserting after paragraph (6)
20 the following:

21 “(7) a secure process for providing the status
22 of every remedial action and unremediated identified
23 system vulnerability of a high value asset to the Di-
24 rector and the Director of the Cybersecurity and In-
25 frastructure Security Agency, using automation and

1 machine-readable data to the greatest extent prac-
2 ticable;” and

3 (vi) in paragraph (8)(C), as so redesi-
4 gnated—

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

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

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

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

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

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

20 (aa) in subclause (II), by
21 adding “and” at the end;

22 (bb) by striking subclause
23 (III); and

1 (cc) by redesignating sub-
2 clause (IV) as subclause (III);
3 and

4 (C) in subsection (c)—

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

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

9 “(1) BIENNIAL REPORT.—Not later than 2
10 years after the date of enactment of the Federal In-
11 formation Security Modernization Act of 2023 and
12 not less frequently than once every 2 years there-
13 after, using the continuous and ongoing agency sys-
14 tem risk assessment required under subsection
15 (a)(1)(A), the head of each agency shall submit to
16 the Director, the National Cyber Director, the Di-
17 rector of the Cybersecurity and Infrastructure Secu-
18 rity Agency, the Comptroller General of the United
19 States, the majority and minority leaders of the Sen-
20 ate, the Speaker and minority leader of the House
21 of Representatives, the Committee on Homeland Se-
22 curity and Governmental Affairs of the Senate, the
23 Committee on Oversight and Accountability of the
24 House of Representatives, the Committee on Home-
25 land Security of the House of Representatives, the

1 Committee on Commerce, Science, and Transpor-
2 tation of the Senate, the Committee on Science,
3 Space, and Technology of the House of Representa-
4 tives, and the appropriate authorization and appro-
5 priations committees of Congress a report that—

6 “(A) summarizes the agency system risk
7 assessment required under subsection (a)(1)(A);

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

18 “(C) summarizes the status of remedial ac-
19 tions identified by inspector general of the
20 agency, the Comptroller General of the United
21 States, and any other source determined appro-
22 priate by the head of the agency.

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

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

4 “(B) may include 1 or more annexes that
5 contain classified or other sensitive information,
6 as appropriate.

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

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

19 (4) in section 3555—

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

23 (B) in subsection (a)—

24 (i) in paragraph (1), by inserting
25 “during which a report is required to be

1 submitted under section 3553(c),” after
2 “Each year”;

3 (ii) in paragraph (2)(A), by inserting
4 “, including by performing, or reviewing
5 the results of, agency penetration testing
6 and analyzing the vulnerability disclosure
7 program of the agency” after “information
8 systems”; and

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

11 “(3) An evaluation under this section may in-
12 clude recommendations for improving the cybersecu-
13 rity posture of the agency.”;

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

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

19 (E) in subsection (g)(2)—

20 (i) by striking “this subsection shall”
21 and inserting “this subsection—
22 “(A) shall”;

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

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

3 “(B) identify any entity that performs an
4 independent evaluation under subsection (b).”;
5 and

6 (F) by striking subsection (j) and inserting
7 the following:

8 “(j) GUIDANCE.—

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

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

20 “(A) the identification of the most common
21 successful threat patterns;

22 “(B) the identification of security controls
23 that address the threat patterns described in
24 subparagraph (A);

1 “(C) any other security risks unique to
2 Federal systems; and

3 “(D) any other element the Director deter-
4 mines appropriate.”; and
5 (5) in section 3556(a)—

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

10 (B) in paragraph (4), by striking
11 “3554(b)” and inserting “3554(a)(1)(A)”.

12 (d) CONFORMING AMENDMENTS.—

13 (1) TABLE OF SECTIONS.—The table of sections
14 for chapter 35 of title 44, United States Code, is
15 amended by striking the item relating to section
16 3555 and inserting the following:

“3555. Independent evaluation.”.

17 (2) OMB REPORTS.—Section 226(e) of the Cy-
18 bersecurity Act of 2015 (6 U.S.C. 1524(e)) is
19 amended—

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

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

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

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

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

15 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

19 “SUBCHAPTER IV—FEDERAL SYSTEM
 20 INCIDENT RESPONSE

21 “§ 3591. Definitions

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

1 “(b) ADDITIONAL DEFINITIONS.—As used in this
2 subchapter:

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

5 “(A) the majority and minority leaders of
6 the Senate;

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

9 “(C) the Committee on Homeland Security
10 and Governmental Affairs of the Senate;

11 “(D) the Committee on Commerce,
12 Science, and Transportation of the Senate;

13 “(E) the Committee on Oversight and Ac-
14 countability of the House of Representatives;

15 “(F) the Committee on Homeland Security
16 of the House of Representatives;

17 “(G) the Committee on Science, Space,
18 and Technology of the House of Representa-
19 tives;

20 “(H) the appropriate authorization and ap-
21 propriations committees of Congress;

22 “(I) the Director;

23 “(J) the Director of the Cybersecurity and
24 Infrastructure Security Agency;

25 “(K) the National Cyber Director;

1 “(L) the Comptroller General of the
2 United States; and

3 “(M) the inspector general of any impacted
4 agency.

5 “(2) AWARDEE.—The term ‘awardee’, with re-
6 spect to an agency—

7 “(A) means—

8 “(i) the recipient of a grant from an
9 agency;

10 “(ii) a party to a cooperative agree-
11 ment with an agency; and

12 “(iii) a party to an other transaction
13 agreement with an agency; and

14 “(B) includes a subawardee of an entity
15 described in subparagraph (A).

16 “(3) BREACH.—The term ‘breach’—

17 “(A) means the compromise, unauthorized
18 disclosure, unauthorized acquisition, or loss of
19 control of personally identifiable information or
20 any similar occurrence; and

21 “(B) includes any additional meaning
22 given the term in policies, principles, standards,
23 or guidelines issued by the Director.

24 “(4) CONTRACTOR.—The term ‘contractor’
25 means a prime contractor of an agency or a subcon-

1 tractor of a prime contractor of an agency that cre-
2 ates, collects, stores, processes, maintains, or trans-
3 mits Federal information on behalf of an agency.

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

9 “(6) FEDERAL INFORMATION SYSTEM.—The
10 term ‘Federal information system’ means an infor-
11 mation system owned, managed, or operated by an
12 agency, or on behalf of an agency by a contractor,
13 an awardee, or another organization.

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

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

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

1 **“§ 3592. Notification of breach**

2 “(a) DEFINITION.—In this section, the term ‘covered
3 breach’ means a breach—

4 “(1) involving not less than 50,000 potentially
5 affected individuals; or

6 “(2) the result of which the head of an agency
7 determines that notifying potentially affected indi-
8 viduals is necessary pursuant to subsection (b)(1),
9 regardless of whether—

10 “(A) the number of potentially affected in-
11 dividuals is less than 50,000; or

12 “(B) the notification is delayed under sub-
13 section (d).

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

20 “(1) determine whether notice to any individual
21 potentially affected by the breach is appropriate, in-
22 cluding by conducting an assessment of the risk of
23 harm to the individual that considers—

24 “(A) the nature and sensitivity of the per-
25 sonally identifiable information affected by the
26 breach;

1 “(B) the likelihood of access to and use of
2 the personally identifiable information affected
3 by the breach;

4 “(C) the type of breach; and

5 “(D) any other factors determined by the
6 Director; and

7 “(2) if the head of the agency determines notifi-
8 cation is necessary pursuant to paragraph (1), pro-
9 vide written notification in accordance with sub-
10 section (c) to each individual potentially affected by
11 the breach—

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

14 “(B) through an appropriate alternative
15 method of notification.

16 “(c) CONTENTS OF NOTIFICATION.—Each notifica-
17 tion of a breach provided to an individual under subsection
18 (b)(2) shall include, to the maximum extent practicable—

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

20 “(2) if possible, a description of the types of
21 personally identifiable information affected by the
22 breach;

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

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

3 “(B) may include a telephone number,
4 mailing address, or a website;

5 “(4) information on any remedy being offered
6 by the agency;

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

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

17 “(d) DELAY OF NOTIFICATION.—

18 “(1) IN GENERAL.—The head of an agency, in
19 coordination with the Director and the National
20 Cyber Director, and as appropriate, the Attorney
21 General, the Director of National Intelligence, or the
22 Secretary of Homeland Security, may delay a notifi-
23 cation required under subsection (b) or (e) if the no-
24 tification would—

1 “(A) impede a criminal investigation or a
2 national security activity;

3 “(B) cause an adverse result (as described
4 in section 2705(a)(2) of title 18);

5 “(C) reveal sensitive sources and methods;

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

7 “(E) hamper security remediation actions.

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

10 “(3) NATIONAL SECURITY SYSTEMS.—The head
11 of an agency delaying notification under this sub-
12 section with respect to a breach exclusively of a na-
13 tional security system shall coordinate such delay
14 with the Secretary of Defense.

15 “(e) UPDATE NOTIFICATION.—If an agency deter-
16 mines there is a significant change in the reasonable basis
17 to conclude that a breach occurred, a significant change
18 to the determination made under subsection (b)(1), or that
19 it is necessary to update the details of the information pro-
20 vided to potentially affected individuals as described in
21 subsection (c), the agency shall as expeditiously as prac-
22 ticable and without unreasonable delay, and in any case
23 not later than 30 days after such a determination, notify
24 each individual who received a notification pursuant to
25 subsection (b) of those changes.

1 “(f) DELAY OF NOTIFICATION REPORT.—

2 “(1) IN GENERAL.—Not later than 1 year after
3 the date of enactment of the Federal Information
4 Security Modernization Act of 2023, and annually
5 thereafter, the head of an agency, in coordination
6 with any official who delays a notification under sub-
7 section (d), shall submit to the appropriate reporting
8 entities a report on each delay that occurred during
9 the previous 2 years.

10 “(2) COMPONENT OF OTHER REPORT.—The
11 head of an agency may submit the report required
12 under paragraph (1) as a component of the report
13 submitted under section 3554(c).

14 “(g) CONGRESSIONAL REPORTING REQUIRE-
15 MENTS.—

16 “(1) REVIEW AND UPDATE.—On a periodic
17 basis, the Director of the Office of Management and
18 Budget shall review, and update as appropriate,
19 breach notification policies and guidelines for agen-
20 cies.

21 “(2) REQUIRED NOTICE FROM AGENCIES.—
22 Subject to paragraph (4), the Director of the Office
23 of Management and Budget shall require the head
24 of an agency affected by a covered breach to expedi-
25 tiously and not later than 30 days after the date on

1 which the agency discovers the covered breach give
2 notice of the breach, which may be provided elec-
3 tronically, to—

4 “(A) each congressional committee de-
5 scribed in section 3554(c)(1); and

6 “(B) the Committee on the Judiciary of
7 the Senate and the Committee on the Judiciary
8 of the House of Representatives.

9 “(3) CONTENTS OF NOTICE.—Notice of a cov-
10 ered breach provided by the head of an agency pur-
11 suant to paragraph (2) shall include, to the extent
12 practicable—

13 “(A) information about the covered breach,
14 including a summary of any information about
15 how the covered breach occurred known by the
16 agency as of the date of the notice;

17 “(B) an estimate of the number of individ-
18 uals affected by the covered breach based on in-
19 formation known by the agency as of the date
20 of the notice, including an assessment of the
21 risk of harm to affected individuals;

22 “(C) a description of any circumstances
23 necessitating a delay in providing notice to indi-
24 viduals affected by the covered breach in ac-
25 cordance with subsection (d); and

1 “(D) an estimate of when the agency will
2 provide notice to individuals affected by the cov-
3 ered breach, if applicable.

4 “(4) EXCEPTION.—Any agency that is required
5 to provide notice to Congress pursuant to paragraph
6 (2) due to a covered breach exclusively on a national
7 security system shall only provide such notice to—

8 “(A) the majority and minority leaders of
9 the Senate;

10 “(B) the Speaker and minority leader of
11 the House of Representatives;

12 “(C) the appropriations committees of
13 Congress;

14 “(D) the Committee on Homeland Security
15 and Governmental Affairs of the Senate;

16 “(E) the Select Committee on Intelligence
17 of the Senate;

18 “(F) the Committee on Oversight and Ac-
19 countability of the House of Representatives;
20 and

21 “(G) the Permanent Select Committee on
22 Intelligence of the House of Representatives.

23 “(5) RULE OF CONSTRUCTION.—Nothing in
24 paragraphs (1) through (3) shall be construed to
25 alter any authority of an agency.

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

3 “(1) limit—

4 “(A) the authority of the Director to issue
5 guidance relating to notifications of, or the
6 head of an agency to notify individuals poten-
7 tially affected by, breaches that are not deter-
8 mined to be covered breaches or major inci-
9 dents;

10 “(B) the authority of the Director to issue
11 guidance relating to notifications and reporting
12 of breaches, covered breaches, or major inci-
13 dents;

14 “(C) the authority of the head of an agen-
15 cy to provide more information than required
16 under subsection (b) when notifying individuals
17 potentially affected by a breach;

18 “(D) the timing of incident reporting or
19 the types of information included in incident re-
20 ports provided, pursuant to this subchapter,
21 to—

22 “(i) the Director;

23 “(ii) the National Cyber Director;

24 “(iii) the Director of the Cybersecu-
25 rity and Infrastructure Security Agency; or

1 “(iv) any other agency;

2 “(E) the authority of the head of an agen-
3 cy to provide information to Congress about
4 agency breaches, including—

5 “(i) breaches that are not covered
6 breaches; and

7 “(ii) additional information beyond
8 the information described in subsection
9 (g)(3); or

10 “(F) any congressional reporting require-
11 ments of agencies under any other law; or

12 “(2) limit or supersede any existing privacy
13 protections in existing law.

14 **“§ 3593. Congressional and executive branch reports**
15 **on major incidents**

16 “(a) APPROPRIATE CONGRESSIONAL ENTITIES.—In
17 this section, the term ‘appropriate congressional entities’
18 means—

19 “(1) the majority and minority leaders of the
20 Senate;

21 “(2) the Speaker and minority leader of the
22 House of Representatives;

23 “(3) the Committee on Homeland Security and
24 Governmental Affairs of the Senate;

1 “(4) the Committee on Commerce, Science, and
2 Transportation of the Senate;

3 “(5) the Committee on Oversight and Account-
4 ability of the House of Representatives;

5 “(6) the Committee on Homeland Security of
6 the House of Representatives;

7 “(7) the Committee on Science, Space, and
8 Technology of the House of Representatives; and

9 “(8) the appropriate authorization and appro-
10 priations committees of Congress.

11 “(b) INITIAL NOTIFICATION.—

12 “(1) IN GENERAL.—Not later than 72 hours
13 after an agency has a reasonable basis to conclude
14 that a major incident occurred, the head of the
15 agency impacted by the major incident shall submit
16 to the appropriate reporting entities a written notifi-
17 cation, which may be submitted electronically and
18 include 1 or more annexes that contain classified or
19 other sensitive information, as appropriate.

20 “(2) CONTENTS.—A notification required under
21 paragraph (1) with respect to a major incident shall
22 include the following, based on information available
23 to agency officials as of the date on which the agen-
24 cy submits the notification:

1 “(A) A summary of the information avail-
2 able about the major incident, including how
3 the major incident occurred and the threat
4 causing the major incident.

5 “(B) If applicable, information relating to
6 any breach associated with the major incident,
7 regardless of whether—

8 “(i) the breach was the reason the in-
9 cident was determined to be a major inci-
10 dent; and

11 “(ii) head of the agency determined it
12 was appropriate to provide notification to
13 potentially impacted individuals pursuant
14 to section 3592(b)(1).

15 “(C) A preliminary assessment of the im-
16 pacts to—

17 “(i) the agency;

18 “(ii) the Federal Government;

19 “(iii) the national security, foreign re-
20 lations, homeland security, and economic
21 security of the United States; and

22 “(iv) the civil liberties, public con-
23 fidence, privacy, and public health and
24 safety of the people of the United States.

1 “(D) If applicable, whether any ransom
2 has been demanded or paid, or is expected to be
3 paid, by any entity operating a Federal infor-
4 mation system or with access to Federal infor-
5 mation or a Federal information system, includ-
6 ing, as available, the name of the entity de-
7 manding ransom, the date of the demand, and
8 the amount and type of currency demanded, un-
9 less disclosure of such information will disrupt
10 an active Federal law enforcement or national
11 security operation.

12 “(c) SUPPLEMENTAL UPDATE.—Within a reasonable
13 amount of time, but not later than 30 days after the date
14 on which the head of an agency submits a written notifica-
15 tion under subsection (a), the head of the agency shall
16 provide to the appropriate congressional entities an un-
17 classified and written update, which may include 1 or
18 more annexes that contain classified or other sensitive in-
19 formation, as appropriate, on the major incident, based
20 on information available to agency officials as of the date
21 on which the agency provides the update, on—

22 “(1) system vulnerabilities relating to the major
23 incident, where applicable, means by which the
24 major incident occurred, the threat causing the

1 major incident, where applicable, and impacts of the
2 major incident to—

3 “(A) the agency;

4 “(B) other Federal agencies, Congress, or
5 the judicial branch;

6 “(C) the national security, foreign rela-
7 tions, homeland security, or economic security
8 of the United States; or

9 “(D) the civil liberties, public confidence,
10 privacy, or public health and safety of the peo-
11 ple of the United States;

12 “(2) the status of compliance of the affected
13 Federal information system with applicable security
14 requirements at the time of the major incident;

15 “(3) if the major incident involved a breach, a
16 description of the affected information, an estimate
17 of the number of individuals potentially impacted,
18 and any assessment to the risk of harm to such indi-
19 viduals;

20 “(4) an update to the assessment of the risk to
21 agency operations, or to impacts on other agency or
22 non-Federal entity operations, affected by the major
23 incident; and

24 “(5) the detection, response, and remediation
25 actions of the agency, including any support pro-

1 vided by the Cybersecurity and Infrastructure Secu-
2 rity Agency under section 3594(d), if applicable.

3 “(d) ADDITIONAL UPDATE.—If the head of an agen-
4 cy, the Director, or the National Cyber Director deter-
5 mines that there is any significant change in the under-
6 standing of the scope, scale, or consequence of a major
7 incident for which the head of the agency submitted a
8 written notification and update under subsections (b) and
9 (c), the head of the agency shall submit to the appropriate
10 congressional entities a written update that includes infor-
11 mation relating to the change in understanding.

12 “(e) BIENNIAL REPORT.—Each agency shall submit
13 as part of the biennial report required under section
14 3554(c)(1) a description of each major incident that oc-
15 curred during the 2-year period preceding the date on
16 which the biennial report is submitted.

17 “(f) REPORT DELIVERY.—

18 “(1) IN GENERAL.—Any written notification or
19 update required to be submitted under this section—

20 “(A) shall be submitted in an electronic
21 format; and

22 “(B) may be submitted in a paper format.

23 “(2) CLASSIFICATION STATUS.—Any written
24 notification or update required to be submitted
25 under this section—

1 “(A) shall be—

2 “(i) unclassified; and

3 “(ii) submitted through unclassified
4 electronic means pursuant to paragraph
5 (1)(A); and

6 “(B) may include classified annexes, as ap-
7 propriate.

8 “(g) REPORT CONSISTENCY.—To achieve consistent
9 and coherent agency reporting to Congress, the National
10 Cyber Director, in coordination with the Director, shall—

11 “(1) provide recommendations to agencies on
12 formatting and the contents of information to be in-
13 cluded in the reports required under this section, in-
14 cluding recommendations for consistent formats for
15 presenting any associated metrics; and

16 “(2) maintain a comprehensive record of each
17 major incident notification, update, and briefing pro-
18 vided under this section, which shall—

19 “(A) include, at a minimum—

20 “(i) the full contents of the written
21 notification or update;

22 “(ii) the identity of the reporting
23 agency; and

24 “(iii) the date of submission; and

1 “(iv) a list of the recipient congres-
2 sional entities; and

3 “(B) be made available upon request to the
4 majority and minority leaders of the Senate, the
5 Speaker and minority leader of the House of
6 Representatives, the Committee on Homeland
7 Security and Governmental Affairs of the Sen-
8 ate, and the Committee on Oversight and Ac-
9 countability of the House of Representatives.

10 “(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL
11 REPORTING EXEMPTION.—With respect to a major inci-
12 dent that occurs exclusively on a national security system,
13 the head of the affected agency shall submit the notifica-
14 tions and reports required to be submitted to Congress
15 under this section only to—

16 “(1) the majority and minority leaders of the
17 Senate;

18 “(2) the Speaker and minority leader of the
19 House of Representatives;

20 “(3) the appropriations committees of Con-
21 gress;

22 “(4) the appropriate authorization committees
23 of Congress;

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

1 “(6) the Select Committee on Intelligence of the
2 Senate;

3 “(7) the Committee on Oversight and Account-
4 ability of the House of Representatives; and

5 “(8) the Permanent Select Committee on Intel-
6 ligence of the House of Representatives.

7 “(i) MAJOR INCIDENTS INCLUDING BREACHES.—If
8 a major incident constitutes a covered breach, as defined
9 in section 3592(a), information on the covered breach re-
10 quired to be submitted to Congress pursuant to section
11 3592(g) may—

12 “(1) be included in the notifications required
13 under subsection (b) or (c); or

14 “(2) be reported to Congress under the process
15 established under section 3592(g).

16 “(j) RULE OF CONSTRUCTION.—Nothing in this sec-
17 tion shall be construed to—

18 “(1) limit—

19 “(A) the ability of an agency to provide ad-
20 ditional reports or briefings to Congress;

21 “(B) Congress from requesting additional
22 information from agencies through reports,
23 briefings, or other means;

24 “(C) any congressional reporting require-
25 ments of agencies under any other law; or

1 “(2) limit or supersede any privacy protections
2 under any other law.

3 **“§ 3594. Government information sharing and inci-**
4 **dent response**

5 “(a) IN GENERAL.—

6 “(1) INCIDENT SHARING.—Subject to para-
7 graph (4) and subsection (b), and in accordance
8 with the applicable requirements pursuant to section
9 3553(b)(2)(A) for reporting to the Federal informa-
10 tion security incident center established under sec-
11 tion 3556, the head of each agency shall provide to
12 the Cybersecurity and Infrastructure Security Agen-
13 cy information relating to any incident affecting the
14 agency, whether the information is obtained by the
15 Federal Government directly or indirectly.

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 include, at a min-
19 imum—

20 “(A) a full description of the incident, in-
21 cluding—

22 “(i) all indicators of compromise and
23 tactics, techniques, and procedures;

24 “(ii) an indicator of how the intruder
25 gained initial access, accessed agency data

1 or systems, and undertook additional ac-
2 tions on the network of the agency;

3 “(iii) information that would support
4 enabling defensive measures; and

5 “(iv) other information that may as-
6 sist in identifying other victims;

7 “(B) information to help prevent similar
8 incidents, such as information about relevant
9 safeguards in place when the incident occurred
10 and the effectiveness of those safeguards; and

11 “(C) information to aid in incident re-
12 sponse, such as—

13 “(i) a description of the affected sys-
14 tems or networks;

15 “(ii) the estimated dates of when the
16 incident occurred; and

17 “(iii) information that could reason-
18 ably help identify any malicious actor that
19 may have conducted or caused the inci-
20 dent, subject to appropriate privacy protec-
21 tions.

22 “(3) INFORMATION SHARING.—The Director of
23 the Cybersecurity and Infrastructure Security Agen-
24 cy shall—

1 “(A) make incident information provided
2 under paragraph (1) available to the Director
3 and the National Cyber Director;

4 “(B) to the greatest extent practicable,
5 share information relating to an incident with—

6 “(i) the head of any agency that may
7 be—

8 “(I) impacted by the incident;

9 “(II) particularly susceptible to
10 the incident; or

11 “(III) similarly targeted by the
12 incident; and

13 “(ii) appropriate Federal law enforce-
14 ment agencies to facilitate any necessary
15 threat response activities, as requested;

16 “(C) coordinate any necessary information
17 sharing efforts relating to a major incident with
18 the private sector; and

19 “(D) notify the National Cyber Director of
20 any efforts described in subparagraph (C).

21 “(4) NATIONAL SECURITY SYSTEMS EXEMP-
22 TION.—

23 “(A) IN GENERAL.—Notwithstanding
24 paragraphs (1) and (3), each agency operating
25 or exercising control of a national security sys-

1 tem shall share information about an incident
2 that occurs exclusively on a national security
3 system with the Secretary of Defense, the Di-
4 rector, the National Cyber Director, and the
5 Director of the Cybersecurity and Infrastruc-
6 ture Security Agency to the extent consistent
7 with standards and guidelines for national secu-
8 rity systems issued in accordance with law and
9 as directed by the President.

10 “(B) PROTECTIONS.—Any information
11 sharing and handling of information under this
12 paragraph shall be appropriately protected con-
13 sistent with procedures authorized for the pro-
14 tection of sensitive sources and methods or by
15 procedures established for information that
16 have been specifically authorized under criteria
17 established by an Executive order or an Act of
18 Congress to be kept classified in the interest of
19 national defense or foreign policy.

20 “(b) AUTOMATION.—In providing information and
21 selecting a method to provide information under sub-
22 section (a), the head of each agency shall implement sub-
23 section (a)(1) in a manner that provides such information
24 to the Cybersecurity and Infrastructure Security Agency

1 in an automated and machine-readable format, to the
2 greatest extent practicable.

3 “(c) INCIDENT RESPONSE.—Each agency that has a
4 reasonable basis to suspect or conclude that a major inci-
5 dent occurred involving Federal information in electronic
6 medium or form that does not exclusively involve a na-
7 tional security system shall coordinate with—

8 “(1) the Cybersecurity and Infrastructure Secu-
9 rity Agency to facilitate asset response activities and
10 provide recommendations for mitigating future inci-
11 dents; and

12 “(2) consistent with relevant policies, appro-
13 priate Federal law enforcement agencies to facilitate
14 threat response activities.

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

16 “(a) REPORTING.—

17 “(1) IN GENERAL.—Any contractor or awardee
18 of an agency shall report to the agency if the con-
19 tractor or awardee has a reasonable basis to con-
20 clude that—

21 “(A) an incident or breach has occurred
22 with respect to Federal information the con-
23 tractor or awardee collected, used, or main-
24 tained on behalf of an agency;

1 “(B) an incident or breach has occurred
2 with respect to a Federal information system
3 used, operated, managed, or maintained on be-
4 half of an agency by the contractor or awardee;

5 “(C) a component of any Federal informa-
6 tion system operated, managed, or maintained
7 by a contractor or awardee contains a security
8 vulnerability, including a supply chain com-
9 promise or an identified software or hardware
10 vulnerability, for which there is reliable evidence
11 of attempted or successful exploitation of the
12 vulnerability by an actor without authorization
13 of the Federal information system owner; or

14 “(D) the contractor or awardee has re-
15 ceived personally identifiable information, per-
16 sonal health information, or other clearly sen-
17 sitive information that is beyond the scope of
18 the contract or agreement with the agency from
19 the agency that the contractor or awardee is
20 not authorized to receive.

21 “(2) THIRD-PARTY REPORTS OF
22 VULNERABILITIES.—Subject to the guidance issued
23 by the Director pursuant to paragraph (4), any con-
24 tractor or awardee of an agency shall report to the
25 agency and the Cybersecurity and Infrastructure Se-

1 security Agency if the contractor or awardee has a
2 reasonable basis to suspect or conclude that a com-
3 ponent of any Federal information system operated,
4 managed, or maintained on behalf of an agency by
5 the contractor or awardee on behalf of the agency
6 contains a security vulnerability, including a supply
7 chain compromise or an identified software or hard-
8 ware vulnerability, that has been reported to the
9 contractor or awardee by a third party, including
10 through a vulnerability disclosure program.

11 “(3) PROCEDURES.—

12 “(A) SHARING WITH CISA.—As soon as
13 practicable following a report of an incident to
14 an agency by a contractor or awardee under
15 paragraph (1), the head of the agency shall pro-
16 vide, pursuant to section 3594, information
17 about the incident to the Director of the Cyber-
18 security and Infrastructure Security Agency.

19 “(B) TIME FOR REPORTING.—Unless a
20 different time for reporting is specified in a
21 contract, grant, cooperative agreement, or other
22 transaction agreement, a contractor or awardee
23 shall—

24 “(i) make a report required under
25 paragraph (1) not later than 1 day after

1 the date on which the contractor or award-
2 ee has reasonable basis to suspect or con-
3 clude that the criteria under paragraph (1)
4 have been met; and

5 “(ii) make a report required under
6 paragraph (2) within a reasonable time,
7 but not later than 90 days after the date
8 on which the contractor or awardee has
9 reasonable basis to suspect or conclude
10 that the criteria under paragraph (2) have
11 been met.

12 “(C) PROCEDURES.—Following a report of
13 a breach or incident to an agency by a con-
14 tractor or awardee under paragraph (1), the
15 head of the agency, in consultation with the
16 contractor or awardee, shall carry out the appli-
17 cable requirements under sections 3592, 3593,
18 and 3594 with respect to the breach or inci-
19 dent.

20 “(D) RULE OF CONSTRUCTION.—Nothing
21 in subparagraph (B) shall be construed to allow
22 the negation of the requirements to report
23 vulnerabilities under paragraph (1) or (2)
24 through a contract, grant, cooperative agree-
25 ment, or other transaction agreement.

1 “(4) GUIDANCE.—The Director shall issue
2 guidance to agencies relating to the scope of
3 vulnerabilities to be reported under paragraph (2),
4 such as the minimum severity of a vulnerability re-
5 quired to be reported or whether vulnerabilities that
6 are already publicly disclosed must be reported.

7 “(b) REGULATIONS; MODIFICATIONS.—

8 “(1) IN GENERAL.—Not later than 1 year after
9 the date of enactment of the Federal Information
10 Security Modernization Act of 2023—

11 “(A) the Federal Acquisition Regulatory
12 Council shall promulgate regulations, as appro-
13 priate, relating to the responsibilities of con-
14 tractors and recipients of other transaction
15 agreements and cooperative agreements to com-
16 ply with this section; and

17 “(B) the Office of Federal Financial Man-
18 agement shall promulgate regulations under
19 title 2, Code of Federal Regulations, as appro-
20 priate, relating to the responsibilities of grant-
21 ees to comply with this section.

22 “(2) IMPLEMENTATION.—Not later than 1 year
23 after the date on which the Federal Acquisition Reg-
24 ulatory Council and the Office of Federal Financial
25 Management promulgates regulations under para-

1 graph (1), the head of each agency shall implement
2 policies and procedures, as appropriate, necessary to
3 implement those regulations.

4 “(3) CONGRESSIONAL NOTIFICATION.—

5 “(A) IN GENERAL.—The head of each
6 agency head shall notify the Director upon im-
7 plementation of policies and procedures nec-
8 essary to implement the regulations promul-
9 gated under paragraph (1).

10 “(B) OMB NOTIFICATION.— Not later
11 than 30 days after the date described in para-
12 graph (2), the Director shall notify the Com-
13 mittee on Homeland Security and Govern-
14 mental Affairs of the Senate and the Commit-
15 tees on Oversight and Accountability and
16 Homeland Security of the House of Representa-
17 tives on the status of the implementation by
18 each agency of the regulations promulgated
19 under paragraph (1).

20 “(c) NATIONAL SECURITY SYSTEMS EXEMPTION.—

21 Notwithstanding any other provision of this section, a con-
22 tractor or awardee of an agency that would be required
23 to report an incident or vulnerability pursuant to this sec-
24 tion that occurs exclusively on a national security system
25 shall—

1 “(1) report the incident or vulnerability to the
2 head of the agency and the Secretary of Defense;
3 and

4 “(2) comply with applicable laws and policies
5 relating to national security systems.

6 **“§ 3596. Training**

7 “(a) COVERED INDIVIDUAL DEFINED.—In this sec-
8 tion, the term ‘covered individual’ means an individual
9 who obtains access to a Federal information system be-
10 cause of the status of the individual as—

11 “(1) an employee, contractor, awardee, volun-
12 teer, or intern of an agency; or

13 “(2) an employee of a contractor or awardee of
14 an agency.

15 “(b) BEST PRACTICES AND CONSISTENCY.—The Di-
16 rector of the Cybersecurity and Infrastructure Security
17 Agency, in consultation with the Director, the National
18 Cyber Director, and the Director of the National Institute
19 of Standards and Technology, shall develop best practices
20 to support consistency across agencies in cybersecurity in-
21 cident response training, including—

22 “(1) information to be collected and shared
23 with the Cybersecurity and Infrastructure Security
24 Agency pursuant to section 3594(a) and processes
25 for sharing such information; and

1 “(2) appropriate training and qualifications for
2 cyber incident responders.

3 “(c) AGENCY TRAINING.—The head of each agency
4 shall develop training for covered individuals on how to
5 identify and respond to an incident, including—

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

8 “(2) the obligation of a covered individual to re-
9 port to the agency any suspected or confirmed inci-
10 dent involving Federal information in any medium
11 or form, including paper, oral, and electronic.

12 “(d) INCLUSION IN ANNUAL TRAINING.—The train-
13 ing developed under subsection (c) may be included as
14 part of an annual privacy, security awareness, or other
15 appropriate training of an agency.

16 **“§ 3597. Analysis and report on Federal incidents**

17 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

18 “(1) QUANTITATIVE AND QUALITATIVE ANAL-
19 YSES.—The Director of the Cybersecurity and Infra-
20 structure Security Agency shall perform and, in co-
21 ordination with the Director and the National Cyber
22 Director, develop, continuous monitoring and quan-
23 titative and qualitative analyses of incidents at agen-
24 cies, including major incidents, including—

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

1 “(i) attacker tactics, techniques, and
2 procedures; and

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

6 “(B) the scope and scale of incidents at
7 agencies;

8 “(C) common root causes of incidents
9 across multiple agencies;

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

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

16 “(F) trends across multiple agencies to ad-
17 dress intrusion detection and incident response
18 capabilities using the metrics established under
19 section 224(c) of the Cybersecurity Act of 2015
20 (6 U.S.C. 1522(c)).

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

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

1 “(A) IN GENERAL.—The Director of the
2 Cybersecurity and Infrastructure Security
3 Agency shall share on an ongoing basis the
4 analyses and underlying data required under
5 this subsection with agencies, the Director, and
6 the National Cyber Director to—

7 “(i) improve the understanding of cy-
8 bersecurity risk of agencies; and

9 “(ii) support the cybersecurity im-
10 provement efforts of agencies.

11 “(B) FORMAT.—In carrying out subpara-
12 graph (A), the Director of the Cybersecurity
13 and Infrastructure Security Agency shall share
14 the analyses—

15 “(i) in human-readable written prod-
16 ucts; and

17 “(ii) to the greatest extent practicable,
18 in machine-readable formats in order to
19 enable automated intake and use by agen-
20 cies.

21 “(C) EXEMPTION.—This subsection shall
22 not apply to incidents that occur exclusively on
23 national security systems.

24 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—
25 Not later than 2 years after the date of enactment of this

1 section, and not less frequently than annually thereafter,
2 the Director of the Cybersecurity and Infrastructure Secu-
3 rity Agency, in consultation with the Director, the Na-
4 tional Cyber Director and the heads of other agencies, as
5 appropriate, shall submit to the appropriate reporting en-
6 tities a report that includes—

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

10 “(2) the quantitative and qualitative analyses of
11 incidents developed under subsection (a)(1) on an
12 agency-by-agency basis and comprehensively across
13 the Federal Government, including—

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

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

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

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

21 “(B) the total number of incidents of the
22 agency; and

23 “(C) an analysis of the agency’s perform-
24 ance against the metrics established under sec-

1 tion 224(e) of the Cybersecurity Act of 2015 (6
2 U.S.C. 1522(e)).

3 “(c) PUBLICATION.—

4 “(1) IN GENERAL.—The Director of the Cyber-
5 security and Infrastructure Security Agency shall
6 make a version of each report submitted under sub-
7 section (b) publicly available on the website of the
8 Cybersecurity and Infrastructure Security Agency
9 during the year during which the report is sub-
10 mitted.

11 “(2) EXEMPTION.—The publication require-
12 ment under paragraph (1) shall not apply to a por-
13 tion of a report that contains content that should be
14 protected in the interest of national security, as de-
15 termined by the Director, the Director of the Cyber-
16 security and Infrastructure Security Agency, or the
17 National Cyber Director.

18 “(3) LIMITATION ON EXEMPTION.—The exemp-
19 tion under paragraph (2) shall not apply to any
20 version of a report submitted to the appropriate re-
21 porting entities under subsection (b).

22 “(4) REQUIREMENT FOR COMPILING INFORMA-
23 TION.—

24 “(A) COMPILATION.—Subject to subpara-
25 graph (B), in making a report publicly available

1 under paragraph (1), the Director of the Cyber-
2 security and Infrastructure Security Agency
3 shall sufficiently compile information so that no
4 specific incident of an agency can be identified.

5 “(B) EXCEPTION.—The Director of the
6 Cybersecurity and Infrastructure Security
7 Agency may include information that enables a
8 specific incident of an agency to be identified in
9 a publicly available report—

10 “(i) with the concurrence of the Di-
11 rector and the National Cyber Director;

12 “(ii) in consultation with the impacted
13 agency; and

14 “(iii) in consultation with the inspec-
15 tor general of the impacted agency.

16 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

21 “(2) NONCOMPLIANCE REPORTS.—During any
22 year during which the head of an agency does not
23 provide data for an incident to the Cybersecurity
24 and Infrastructure Security Agency in accordance
25 with section 3594(a), the head of the agency, in co-

1 ordination with the Director of the Cybersecurity
2 and Infrastructure Security Agency and the Direc-
3 tor, shall submit to the appropriate reporting enti-
4 ties a report that includes the information described
5 in subsection (b) with respect to the agency.

6 “(e) NATIONAL SECURITY SYSTEM REPORTS.—

7 “(1) IN GENERAL.—Notwithstanding any other
8 provision of this section, the Secretary of Defense, in
9 consultation with the Director, the National Cyber
10 Director, the Director of National Intelligence, and
11 the Director of the Cybersecurity and Infrastructure
12 Security Agency shall annually submit a report that
13 includes the information described in subsection (b)
14 with respect to national security systems, to the ex-
15 tent that the submission is consistent with standards
16 and guidelines for national security systems issued
17 in accordance with law and as directed by the Presi-
18 dent, to—

19 “(A) the majority and minority leaders of
20 the Senate;

21 “(B) the Speaker and minority leader of
22 the House of Representatives;

23 “(C) the Committee on Homeland Security
24 and Governmental Affairs of the Senate;

1 “(D) the Select Committee on Intelligence
2 of the Senate;

3 “(E) the Committee on Armed Services of
4 the Senate;

5 “(F) the Committee on Appropriations of
6 the Senate;

7 “(G) the Committee on Oversight and Ac-
8 countability of the House of Representatives;

9 “(H) the Committee on Homeland Security
10 of the House of Representatives;

11 “(I) the Permanent Select Committee on
12 Intelligence of the House of Representatives;

13 “(J) the Committee on Armed Services of
14 the House of Representatives; and

15 “(K) the Committee on Appropriations of
16 the House of Representatives.

17 “(2) CLASSIFIED FORM.—A report required
18 under paragraph (1) may be submitted in a classi-
19 fied form.

20 **“§ 3598. Major incident definition**

21 “(a) IN GENERAL.—Not later than 1 year after the
22 later of the date of enactment of the Federal Information
23 Security Modernization Act of 2023 and the most recent
24 publication by the Director of guidance to agencies regard-
25 ing major incidents as of the date of enactment of the

1 Federal Information Security Modernization Act of 2023,
2 the Director shall develop, in coordination with the Na-
3 tional Cyber Director, and promulgate guidance on the
4 definition of the term ‘major incident’ for the purposes
5 of subchapter II and this subchapter.

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

9 “(1) include, with respect to any information
10 collected or maintained by or on behalf of an agency
11 or a Federal information system—

12 “(A) any incident the head of the agency
13 determines is likely to result in demonstrable
14 harm to—

15 “(i) the national security interests,
16 foreign relations, homeland security, or
17 economic security of the United States; or

18 “(ii) the civil liberties, public con-
19 fidence, privacy, or public health and safe-
20 ty of the people of the United States;

21 “(B) any incident the head of the agency
22 determines likely to result in an inability or
23 substantial disruption for the agency, a compo-
24 nent of the agency, or the Federal Government,
25 to provide 1 or more critical services;

1 “(C) any incident the head of the agency
2 determines substantially disrupts or substan-
3 tially degrades the operations of a high value
4 asset owned or operated by the agency;

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

11 “(E) any other type of incident determined
12 appropriate by the Director;

13 “(2) stipulate that the National Cyber Director,
14 in consultation with the Director and the Director of
15 the Cybersecurity and Infrastructure Security Agen-
16 cy, may declare a major incident at any agency, and
17 such a declaration shall be considered if it is deter-
18 mined that an incident—

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

20 and

21 “(B) is enabled by—

22 “(i) a common technical root cause,
23 such as a supply chain compromise, or a
24 common software or hardware vulner-
25 ability; or

1 “(ii) the related activities of a com-
2 mon threat actor;

3 “(3) stipulate that, in determining whether an
4 incident constitutes a major incident under the
5 standards described in paragraph (1), the head of
6 the agency shall consult with the National Cyber Di-
7 rector; and

8 “(4) stipulate that the mere report of a vulner-
9 ability discovered or disclosed without a loss of con-
10 fidentiality, integrity, or availability shall not on its
11 own constitute a major incident.

12 “(c) EVALUATION AND UPDATES.—Not later than 60
13 days after the date on which the Director first promul-
14 gates the guidance required under subsection (a), and not
15 less frequently than once during the first 90 days of each
16 evenly numbered Congress thereafter, the Director shall
17 provide to the Committee on Homeland Security and Gov-
18 ernmental Affairs of the Senate and the Committees on
19 Oversight and Accountability and Homeland Security of
20 the House of Representatives a briefing that includes—

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

23 “(2) an evaluation of any necessary updates to
24 the definition of the term ‘major incident’ included
25 in the guidance; 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 on major incidents.

“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. 4. 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, as appro-
8 priate—

9 “(i) a cybersecurity risk management
10 plan; and

11 “(ii) a supply chain risk assessment in
12 accordance with section 1326 of title 41.”;

13 and

14 (3) in subsection (c)—

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

18 (B) in paragraph (5)—

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

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

23 and

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

1 “(C) a senior official from the Cybersecu-
2 rity and Infrastructure Security Agency of the
3 Department of Homeland Security, appointed
4 by the Director.”; and

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

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

10 (1) in section 11302—

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

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

20 (2) in section 11303(b)(2)(B)—

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

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

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

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

4 (c) SUBCHAPTER II.—Subchapter II of chapter 113
5 of subtitle III of title 40, United States Code, is amend-
6 ed—

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

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

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

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

17 **SEC. 5. ACTIONS TO ENHANCE FEDERAL INCIDENT TRANS-**
18 **PARENCY.**

19 (a) RESPONSIBILITIES OF THE CYBERSECURITY AND
20 INFRASTRUCTURE SECURITY AGENCY.—

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

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

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

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

13 (B) provide to the appropriate congress-
14 sional committees a briefing on the plan devel-
15 oped under subparagraph (A).

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

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

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

1 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
2 OFFICE OF MANAGEMENT AND BUDGET.—

3 (1) UPDATING FISMA 2014.—Section 2 of the
4 Federal Information Security Modernization Act of
5 2014 (Public Law 113–283; 128 Stat. 3073) is
6 amended—

7 (A) by striking subsections (b) and (d);
8 and

9 (B) by redesignating subsections (c), (e),
10 and (f) as subsections (b), (c), and (d), respec-
11 tively.

12 (2) INCIDENT DATA SHARING.—

13 (A) IN GENERAL.—The Director, in coordi-
14 nation with the Director of the Cybersecurity
15 and Infrastructure Security Agency, shall de-
16 velop, and as appropriate update, guidance, on
17 the content, timeliness, and format of the infor-
18 mation provided by agencies under section
19 3594(a) of title 44, United States Code, as
20 added by this Act.

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

23 (i) enable the efficient development
24 of—

1 (I) lessons learned and rec-
2 ommendations in responding to, recov-
3 ering from, remediating, and miti-
4 gating future incidents; and

5 (II) the report on Federal inci-
6 dents required under section 3597(b)
7 of title 44, United States Code, as
8 added by this Act; and

9 (ii) include requirements for the time-
10 liness of data production.

11 (C) AUTOMATION.—The Director, in co-
12 ordination with the Director of the Cybersecu-
13 rity and Infrastructure Security Agency, shall
14 promote, as feasible, the use of automation and
15 machine-readable data for data sharing under
16 section 3594(a) of title 44, United States Code,
17 as added by this Act.

18 (3) CONTRACTOR AND AWARDEE GUIDANCE.—

19 (A) IN GENERAL.—Not later than 1 year
20 after the date of enactment of this Act, the Di-
21 rector shall issue guidance to agencies on how
22 to deconflict, to the greatest extent practicable,
23 existing regulations, policies, and procedures re-
24 lating to the responsibilities of contractors and

1 awardees established under section 3595 of title
2 44, United States Code, as added by this Act.

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

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

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

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

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

17 “(13) to another agency, to the extent nec-
18 essary, to assist the recipient agency in responding
19 to an incident (as defined in section 3552 of title
20 44) or breach (as defined in section 3591 of title 44)
21 or to fulfill the information sharing requirements
22 under section 3594 of title 44.”.

1 **SEC. 6. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**
2 **UPDATES.**

3 (a) IN GENERAL.—Not later than 1 year after the
4 date of enactment of this Act, the Director shall issue
5 guidance for agencies on—

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

10 (2) establishing a process for securely providing
11 the status of each remedial action for high value as-
12 sets under section 3554(b)(7) of title 44, United
13 States Code, as amended by this Act, to the Director
14 and the Director of the Cybersecurity and Infra-
15 structure Security Agency using automation and ma-
16 chine-readable data, as practicable, which shall in-
17 clude—

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

20 (B) templates for providing the status of
21 the remedial action.

22 (b) COORDINATION.—The head of each agency shall
23 coordinate with the inspector general of the agency, as ap-
24 plicable, to ensure consistent understanding of agency
25 policies for the purpose of evaluations conducted by the
26 inspector general.

1 **SEC. 7. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SEC-**
2 **TOR ENTITIES IMPACTED BY INCIDENTS.**

3 (a) DEFINITIONS.—In this section:

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

8 (2) SENSITIVE INFORMATION.—The term “sen-
9 sitive information” has the meaning given the term
10 by the Director in guidance issued under subsection
11 (b).

12 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-
13 TITIES.—Not later than 1 year after the date of enact-
14 ment of this Act, the Director shall develop, in consulta-
15 tion with the National Cyber Director, and issue guidance
16 requiring the head of each agency to notify a reporting
17 entity, and take into consideration the need to coordinate
18 with Sector Risk Management Agencies (as defined in sec-
19 tion 2200 of the Homeland Security Act of 2002 (6 U.S.C.
20 650)), as appropriate, of an incident at the agency that
21 is likely to substantially affect—

22 (1) the confidentiality or integrity of sensitive
23 information submitted by the reporting entity to the
24 agency pursuant to a statutory or regulatory re-
25 quirement; or

1 (2) any information system (as defined in sec-
2 tion 3502 of title 44, United States Code) used in
3 the transmission or storage of the sensitive informa-
4 tion described in paragraph (1).

5 **SEC. 8. MOBILE SECURITY BRIEFINGS.**

6 (a) IN GENERAL.—Not later than 180 days after the
7 date of enactment of this Act, the Director shall provide
8 to the appropriate congressional committees—

9 (1) a briefing on the compliance of agencies
10 with the No TikTok on Government Devices Act (44
11 U.S.C. 3553 note; Public Law 117–328); and

12 (2) as a component of the briefing required
13 under paragraph (1), a list of each exception of an
14 agency from the No TikTok on Government Devices
15 Act (44 U.S.C. 3553 note; Public Law 117–328),
16 which may include a classified annex.

17 (b) ADDITIONAL BRIEFING.—Not later than 1 year
18 after the date of the briefing required under subsection
19 (a)(1), the Director shall provide to the appropriate con-
20 gressional committees—

21 (1) a briefing on the compliance of any agency
22 that was not compliant with the No TikTok on Gov-
23 ernment Devices Act (44 U.S.C. 3553 note; Public
24 Law 117–328) at the time of the briefing required
25 under subsection (a)(1); and

1 (2) as a component of the briefing required
2 under paragraph (1), an update to the list required
3 under subsection (a)(2).

4 **SEC. 9. DATA AND LOGGING RETENTION FOR INCIDENT RE-**
5 **SPONSE.**

6 (a) **GUIDANCE.**—Not later than 2 years after the date
7 of enactment of this Act the Director, in consultation with
8 the National Cyber Director and the Director of the Cy-
9 bersecurity and Infrastructure Security Agency, shall up-
10 date guidance to agencies regarding requirements for log-
11 ging, log retention, log management, sharing of log data
12 with other appropriate agencies, or any other logging ac-
13 tivity determined to be appropriate by the Director.

14 (b) **NATIONAL SECURITY SYSTEMS.**—The Secretary
15 of Defense shall issue guidance that meets or exceeds the
16 standards required in guidance issued under subsection
17 (a) for National Security Systems.

18 **SEC. 10. CISA AGENCY LIAISONS.**

19 (a) **IN GENERAL.**—Not later than 120 days after the
20 date of enactment of this Act, the Director of the Cyberse-
21 curity and Infrastructure Security Agency shall assign not
22 less than 1 cybersecurity professional employed by the Cy-
23 bersecurity and Infrastructure Security Agency to be the
24 Cybersecurity and Infrastructure Security Agency liaison
25 to the Chief Information Security Officer of each agency.

1 (b) QUALIFICATIONS.—Each liaison assigned under
2 subsection (a) shall have knowledge of—

- 3 (1) cybersecurity threats facing agencies, in-
4 cluding any specific threats to the assigned agency;
- 5 (2) risk assessments of agency systems; and
- 6 (3) other Federal cybersecurity initiatives.

7 (c) DUTIES.—The duties of each liaison assigned
8 under subsection (a) shall include—

- 9 (1) providing, as requested, assistance and ad-
10 vice to the agency Chief Information Security Offi-
11 cer;
- 12 (2) supporting, as requested, incident response
13 coordination between the assigned agency and the
14 Cybersecurity and Infrastructure Security Agency;
- 15 (3) becoming familiar with assigned agency sys-
16 tems, processes, and procedures to better facilitate
17 support to the agency; and
- 18 (4) other liaison duties to the assigned agency
19 solely in furtherance of Federal cybersecurity or sup-
20 port to the assigned agency as a Sector Risk Man-
21 agement Agency, as assigned by the Director of the
22 Cybersecurity and Infrastructure Security Agency in
23 consultation with the head of the assigned agency.

24 (d) LIMITATION.—A liaison assigned under sub-
25 section (a) shall not be a contractor.

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

4 (f) COORDINATION OF ACTIVITIES.—The Director of
5 the Cybersecurity and Infrastructure Security Agency
6 shall consult with the Director on the execution of the du-
7 ties of the Cybersecurity and Infrastructure Security
8 Agency liaisons to ensure that there is no inappropriate
9 duplication of activities among—

10 (1) Federal cybersecurity support to agencies of
11 the Office of Management and Budget; and

12 (2) the Cybersecurity and Infrastructure Secu-
13 rity Agency liaison.

14 (g) RULE OF CONSTRUCTION.—Nothing in this sec-
15 tion shall be construed to impact the ability of the Director
16 to support agency implementation of Federal cybersecurity
17 requirements pursuant to subchapter II of chapter 35 of
18 title 44, United States Code, as amended by this Act.

19 **SEC. 11. FEDERAL PENETRATION TESTING POLICY.**

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

1 **“§ 3559A. Federal penetration testing**

2 “(a) GUIDANCE.—The Director, in consultation with
3 the Director of the Cybersecurity and Infrastructure Secu-
4 rity Agency, shall issue guidance to agencies that—

5 “(1) requires agencies to perform penetration
6 testing on information systems, as appropriate, in-
7 cluding on high value assets;

8 “(2) provides policies governing the develop-
9 ment of—

10 “(A) rules of engagement for using pene-
11 tration testing; and

12 “(B) procedures to use the results of pene-
13 tration testing to improve the cybersecurity and
14 risk management of the agency;

15 “(3) ensures that operational support or a
16 shared service is available; and

17 “(4) in no manner restricts the authority of the
18 Secretary of Homeland Security or the Director of
19 the Cybersecurity and Infrastructure Agency to con-
20 duct threat hunting pursuant to section 3553 of title
21 44, United States Code, or penetration testing under
22 this chapter.

23 “(b) EXCEPTION FOR NATIONAL SECURITY SYS-
24 TEMS.—The guidance issued under subsection (a) shall
25 not apply to national security systems.

1 “(c) DELEGATION OF AUTHORITY FOR CERTAIN SYS-
2 TEMS.—The authorities of the Director described in sub-
3 section (a) shall be delegated to—

4 “(1) the Secretary of Defense in the case of a
5 system described in section 3553(e)(2); and

6 “(2) the Director of National Intelligence in the
7 case of a system described in section 3553(e)(3).”.

8 (b) EXISTING GUIDANCE.—

9 (1) IN GENERAL.—Compliance with guidance
10 issued by the Director relating to penetration testing
11 before the date of enactment of this Act shall be
12 deemed to be compliant with section 3559A of title
13 44, United States Code, as added by this Act.

14 (2) IMMEDIATE NEW GUIDANCE NOT RE-
15 QUIRED.—Nothing in section 3559A of title 44,
16 United States Code, as added by this Act, shall be
17 construed to require the Director to issue new guid-
18 ance to agencies relating to penetration testing be-
19 fore the date described in paragraph (3).

20 (3) GUIDANCE UPDATES.—Notwithstanding
21 paragraphs (1) and (2), not later than 2 years after
22 the date of enactment of this Act, the Director shall
23 review and, as appropriate, update existing guidance
24 requiring penetration testing by agencies.

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

“3559A. Federal penetration testing.”.

5 (d) PENETRATION TESTING BY THE SECRETARY OF
 6 HOMELAND SECURITY.—Section 3553(b) of title 44,
 7 United States Code, as amended by this Act, is further
 8 amended by inserting after paragraph (8) the following:

9 “(9) performing penetration testing that may
 10 leverage manual expert analysis to identify threats
 11 and vulnerabilities within information systems—

12 “(A) without consent or authorization from
 13 agencies; and

14 “(B) with prior notification to the head of
 15 the agency;”.

16 **SEC. 12. VULNERABILITY DISCLOSURE POLICIES.**

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

20 **“§ 3559B. Federal vulnerability disclosure policies**

21 “(a) PURPOSE; SENSE OF CONGRESS.—

22 “(1) PURPOSE.—The purpose of Federal vul-
 23 nerability disclosure policies is to create a mecha-
 24 nism to enable the public to inform agencies of
 25 vulnerabilities in Federal information systems.

1 “(2) SENSE OF CONGRESS.—It is the sense of
2 Congress that, in implementing the requirements of
3 this section, the Federal Government should take
4 appropriate steps to reduce real and perceived bur-
5 dens in communications between agencies and secu-
6 rity researchers.

7 “(b) DEFINITIONS.—In this section:

8 “(1) CONTRACTOR.—The term ‘contractor’ has
9 the meaning given the term in section 3591.

10 “(2) INTERNET OF THINGS.—The term ‘inter-
11 net of things’ has the meaning given the term in
12 Special Publication 800–213 of the National Insti-
13 tute of Standards and Technology, entitled ‘IoT De-
14 vice Cybersecurity Guidance for the Federal Govern-
15 ment: Establishing IoT Device Cybersecurity Re-
16 quirements’, or any successor document.

17 “(3) SECURITY VULNERABILITY.—The term
18 ‘security vulnerability’ has the meaning given the
19 term in section 102 of the Cybersecurity Information
20 Sharing Act of 2015 (6 U.S.C. 1501).

21 “(4) SUBMITTER.—The term ‘submitter’ means
22 an individual that submits a vulnerability disclosure
23 report pursuant to the vulnerability disclosure proc-
24 ess of an agency.

1 “(5) VULNERABILITY DISCLOSURE REPORT.—

2 The term ‘vulnerability disclosure report’ means a
3 disclosure of a security vulnerability made to an
4 agency by a submitter.

5 “(c) GUIDANCE.—The Director shall issue guidance
6 to agencies that includes—

7 “(1) use of the information system security
8 vulnerabilities disclosure process guidelines estab-
9 lished under section 4(a)(1) of the IoT Cybersecurity
10 Improvement Act of 2020 (15 U.S.C. 278g–
11 3b(a)(1));

12 “(2) direction to not recommend or pursue legal
13 action against a submitter or an individual that con-
14 ducts a security research activity that—

15 “(A) represents a good faith effort to iden-
16 tify and report security vulnerabilities in infor-
17 mation systems; or

18 “(B) otherwise represents a good faith ef-
19 fort to follow the vulnerability disclosure policy
20 of the agency developed under subsection (f)(2);

21 “(3) direction on sharing relevant information
22 in a consistent, automated, and machine-readable
23 manner with the Director of the Cybersecurity and
24 Infrastructure Security Agency;

1 “(4) the minimum scope of agency systems re-
2 quired to be covered by the vulnerability disclosure
3 policy of an agency required under subsection (f)(2),
4 including exemptions under subsection (g);

5 “(5) requirements for providing information to
6 the submitter of a vulnerability disclosure report on
7 the resolution of the vulnerability disclosure report;

8 “(6) a stipulation that the mere identification
9 by a submitter of a security vulnerability, without a
10 significant compromise of confidentiality, integrity,
11 or availability, does not constitute a major incident;
12 and

13 “(7) the applicability of the guidance to inter-
14 net of things devices owned or controlled by an
15 agency.

16 “(d) CONSULTATION.—In developing the guidance re-
17 quired under subsection (c)(3), the Director shall consult
18 with the Director of the Cybersecurity and Infrastructure
19 Security Agency.

20 “(e) RESPONSIBILITIES OF CISA.—The Director of
21 the Cybersecurity and Infrastructure Security Agency
22 shall—

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

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

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

9 “(4) as appropriate, implement the require-
10 ments of this section, in accordance with the author-
11 ity under section 3553(b)(8), as a shared service
12 available to agencies.

13 “(f) RESPONSIBILITIES OF AGENCIES.—

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

20 “(A) an appropriate security contact; and

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

24 “(2) VULNERABILITY DISCLOSURE POLICY.—

25 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, including for internet of things
7 devices owned or controlled by the agency;

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

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

13 “(iv) the disclosure policy for a con-
14 tractor; and

15 “(v) the disclosure policy of the agen-
16 cy for sensitive information;

17 “(B) with respect to a vulnerability disclo-
18 sure report to an agency, describe—

19 “(i) how the submitter should submit
20 the vulnerability disclosure report; and

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

1 “(C) include any other relevant informa-
2 tion; and

3 “(D) be mature in scope and cover every
4 internet accessible information system used or
5 operated by that agency or on behalf of that
6 agency.

7 “(3) IDENTIFIED SECURITY
8 VULNERABILITIES.—The head of each agency
9 shall—

10 “(A) consider security vulnerabilities re-
11 ported in accordance with paragraph (2);

12 “(B) commensurate with the risk posed by
13 the security vulnerability, address such security
14 vulnerability using the security vulnerability
15 management process of the agency; and

16 “(C) in accordance with subsection (c)(5),
17 provide information to the submitter of a vul-
18 nerability disclosure report.

19 “(g) EXEMPTIONS.—

20 “(1) IN GENERAL.—The Director and the head
21 of each agency shall carry out this section in a man-
22 ner consistent with the protection of national secu-
23 rity information.

24 “(2) LIMITATION.—The Director and the head
25 of each agency may not publish under subsection

1 (f)(1) or include in a vulnerability disclosure policy
2 under subsection (f)(2) host names, services, infor-
3 mation systems, or other information that the Direc-
4 tor or the head of an agency, in coordination with
5 the Director and other appropriate heads of agen-
6 cies, determines would—

7 “(A) disrupt a law enforcement investiga-
8 tion;

9 “(B) endanger national security or intel-
10 ligence activities; or

11 “(C) impede national defense activities or
12 military operations.

13 “(3) NATIONAL SECURITY SYSTEMS.—This sec-
14 tion shall not apply to national security systems.

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

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

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

23 “(i) REVISION OF FEDERAL ACQUISITION REGULA-
24 TION.—The Federal Acquisition Regulation shall be re-

1 vised as necessary to implement the provisions under this
2 section.”.

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

“3559B. Federal vulnerability disclosure policies.”.

7 (c) CONFORMING UPDATE AND REPEAL.—

8 (1) GUIDELINES ON THE DISCLOSURE PROCESS
9 FOR SECURITY VULNERABILITIES RELATING TO IN-
10 FORMATION SYSTEMS, INCLUDING INTERNET OF
11 THINGS DEVICES.—Section 5 of the IoT Cybersecu-
12 rity Improvement Act of 2020 (15 U.S.C. 278g–3e)
13 is amended by striking subsections (d) and (e).

14 (2) IMPLEMENTATION AND CONTRACTOR COM-
15 PLIANCE.—The IoT Cybersecurity Improvement Act
16 of 2020 (15 U.S.C. 278g–3a et seq.) is amended—

17 (A) by striking section 6 (15 U.S.C. 278g–
18 3d); and

19 (B) by striking section 7 (15 U.S.C. 278g–
20 3e).

21 **SEC. 13. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

22 (a) BRIEFINGS.—Not later than 1 year after the date
23 of enactment of this Act, the Director shall provide to the
24 Committee on Homeland Security and Governmental Af-
25 fairs of the Senate and the Committees on Oversight and

1 Accountability and Homeland Security of the House of
2 Representatives a briefing on progress in increasing the
3 internal defenses of agency systems, including—

4 (1) shifting away from trusted networks to im-
5 plement security controls based on a presumption of
6 compromise, including through the transition to zero
7 trust architecture;

8 (2) implementing principles of least privilege in
9 administering information security programs;

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

13 (4) identifying incidents quickly;

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

18 (6) otherwise increasing the resource costs for
19 entities that cause incidents to be successful.

20 (b) PROGRESS REPORT.—As a part of each report
21 required to be submitted under section 3553(c) of title 44,
22 United States Code, during the period beginning on the
23 date that is 4 years after the date of enactment of this
24 Act and ending on the date that is 10 years after the date
25 of enactment of this Act, the Director shall include an up-

1 date on agency implementation of zero trust architecture,
2 which shall include—

3 (1) a description of steps agencies have com-
4 pleted, including progress toward achieving any re-
5 quirements issued by the Director, including the
6 adoption of any models or reference architecture;

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

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

12 (c) CLASSIFIED ANNEX.—Each update required
13 under subsection (b) may include 1 or more annexes that
14 contain classified or other sensitive information, as appro-
15 priate.

16 (d) NATIONAL SECURITY SYSTEMS.—

17 (1) BRIEFING.—Not later than 1 year after the
18 date of enactment of this Act, the Secretary of De-
19 fense shall provide to the Committee on Homeland
20 Security and Governmental Affairs of the Senate,
21 the Committee on Oversight and Accountability of
22 the House of Representatives, the Committee on
23 Armed Services of the Senate, the Committee on
24 Armed Services of the House of Representatives, the
25 Select Committee on Intelligence of the Senate, and

1 the Permanent Select Committee on Intelligence of
2 the House of Representatives a briefing on the im-
3 plementation of zero trust architecture with respect
4 to national security systems.

5 (2) PROGRESS REPORT.—Not later than the
6 date on which each update is required to be sub-
7 mitted under subsection (b), the Secretary of De-
8 fense shall submit to the congressional committees
9 described in paragraph (1) a progress report on the
10 implementation of zero trust architecture with re-
11 spect to national security systems.

12 **SEC. 14. AUTOMATION AND ARTIFICIAL INTELLIGENCE.**

13 (a) DEFINITION.—In this section, the term “informa-
14 tion system” has the meaning given the term in section
15 3502 of title 44, United States Code.

16 (b) USE OF ARTIFICIAL INTELLIGENCE.—

17 (1) IN GENERAL.—As appropriate, the Director
18 shall issue guidance on the use of artificial intel-
19 ligence by agencies to improve the cybersecurity of
20 information systems.

21 (2) CONSIDERATIONS.—The Director and head
22 of each agency shall consider the use and capabilities
23 of artificial intelligence systems wherever automation
24 is used in furtherance of the cybersecurity of infor-
25 mation systems.

1 (3) REPORT.—Not later than 1 year after the
2 date of enactment of this Act, and annually there-
3 after until the date that is 5 years after the date of
4 enactment of this Act, the Director shall submit to
5 the appropriate congressional committees a report
6 on the use of artificial intelligence to further the cy-
7 bersecurity of information systems.

8 (c) COMPTROLLER GENERAL REPORTS.—

9 (1) IN GENERAL.—Not later than 2 years after
10 the date of enactment of this Act, the Comptroller
11 General of the United States shall submit to the ap-
12 propriate congressional committees a report on the
13 risks to the privacy of individuals and the cybersecu-
14 rity of information systems associated with the use
15 by Federal agencies of artificial intelligence systems
16 or capabilities.

17 (2) STUDY.—Not later than 2 years after the
18 date of enactment of this Act, the Comptroller Gen-
19 eral of the United States shall perform a study, and
20 submit to the Committees on Homeland Security
21 and Governmental Affairs and Commerce, Science,
22 and Transportation of the Senate and the Commit-
23 tees on Oversight and Accountability, Homeland Se-
24 curity, and Science, Space, and Technology of the
25 House of Representatives a report, on the use of au-

1 “(B) that shall include a dashboard of
2 open information security recommendations
3 identified in the independent evaluations re-
4 quired by section 3555(a) of title 44; and”;
5 (2) by adding at the end the following:

6 “(5) **RULE OF CONSTRUCTION.**—Nothing in
7 this subsection shall be construed to require the pub-
8 lication of information that is exempted from disclo-
9 sure under section 552 of this title.”.

10 **SEC. 17. SECURITY OPERATIONS CENTER SHARED SERV-**
11 **ICE.**

12 (a) **BRIEFING.**—Not later than 180 days after the
13 date of enactment of this Act, the Director of the Cyberse-
14 curity and Infrastructure Security Agency shall provide to
15 the Committee on Homeland Security and Governmental
16 Affairs of the Senate and the Committee on Homeland
17 Security and the Committee on Oversight and Account-
18 ability of the House of Representatives a briefing on—

19 (1) existing security operations center shared
20 services;

21 (2) the capability for such shared service to
22 offer centralized and simultaneous support to mul-
23 tiple agencies;

24 (3) the capability for such shared service to in-
25 tegrate with or support agency threat hunting activi-

1 ties authorized under section 3553 of title 44,
2 United States Code, as amended by this Act;

3 (4) the capability for such shared service to in-
4 tegrate with or support Federal vulnerability man-
5 agement activities; and

6 (5) future plans for expansion and maturation
7 of such shared service.

8 (b) GAO REPORT.—Not less than 540 days after the
9 date of enactment of this Act, the Comptroller General
10 of the United States shall submit to the appropriate con-
11 gressional committees a report on Federal cybersecurity
12 security operations centers that—

13 (1) identifies Federal agency best practices for
14 efficiency and effectiveness;

15 (2) identifies non-Federal best practices used by
16 large entity operations centers and entities providing
17 operation centers as a service; and

18 (3) includes recommendations for the Cyberse-
19 curity and Infrastructure Security Agency and any
20 other relevant agency to improve the efficiency and
21 effectiveness of security operations centers' shared
22 service offerings.

23 **SEC. 18. FEDERAL CYBERSECURITY REQUIREMENTS.**

24 (a) CODIFYING FEDERAL CYBERSECURITY REQUIRE-
25 MENTS IN TITLE 44.—

1 (1) AMENDMENT TO FEDERAL CYBERSECURITY
2 ENHANCEMENT ACT OF 2015.—Section 225 of the
3 Federal Cybersecurity Enhancement Act of 2015 (6
4 U.S.C. 1523) is amended by striking subsections (b)
5 and (c).

6 (2) TITLE 44.—Section 3554 of title 44, United
7 States Code, as amended by this Act, is further
8 amended by adding at the end the following:

9 “(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT
10 AGENCIES.—

11 “(1) IN GENERAL.—Consistent with policies,
12 standards, guidelines, and directives on information
13 security under this subchapter, and except as pro-
14 vided under paragraph (3), the head of each agency
15 shall—

16 “(A) identify sensitive and mission critical
17 data stored by the agency consistent with the
18 inventory required under section 3505(c);

19 “(B) assess access controls to the data de-
20 scribed in subparagraph (A), the need for read-
21 ily accessible storage of the data, and the need
22 of individuals to access the data;

23 “(C) encrypt or otherwise render indeci-
24 pherable to unauthorized users the data de-

1 scribed in subparagraph (A) that is stored on
2 or transiting agency information systems;

3 “(D) implement a single sign-on trusted
4 identity platform for individuals accessing each
5 public website of the agency that requires user
6 authentication, as developed by the Adminis-
7 trator of General Services in collaboration with
8 the Secretary; and

9 “(E) implement identity management con-
10 sistent with section 504 of the Cybersecurity
11 Enhancement Act of 2014 (15 U.S.C. 7464),
12 including multi-factor authentication, for—

13 “(i) remote access to an information
14 system; and

15 “(ii) each user account with elevated
16 privileges on an information system.

17 “(2) PROHIBITION.—

18 “(A) DEFINITION.—In this paragraph, the
19 term ‘internet of things’ has the meaning given
20 the term in section 3559B.

21 “(B) PROHIBITION.—Consistent with poli-
22 cies, standards, guidelines, and directives on in-
23 formation security under this subchapter, and
24 except as provided under paragraph (3), the
25 head of an agency may not procure, obtain,

1 renew a contract to procure or obtain in any
2 amount, notwithstanding section 1905 of title
3 41, United States Code, or use an internet of
4 things device if the Chief Information Officer of
5 the agency determines during a review required
6 under section 11319(b)(1)(C) of title 40 of a
7 contract for an internet of things device that
8 the use of the device prevents compliance with
9 the standards and guidelines developed under
10 section 4 of the IoT Cybersecurity Improvement
11 Act (15 U.S.C. 278g–3b) with respect to the
12 device.

13 “(3) EXCEPTION.—The requirements under
14 paragraph (1) shall not apply to an information sys-
15 tem for which—

16 “(A) the head of the agency, without dele-
17 gation, has certified to the Director with par-
18 ticularity that—

19 “(i) operational requirements articu-
20 lated in the certification and related to the
21 information system would make it exces-
22 sively burdensome to implement the cyber-
23 security requirement;

24 “(ii) the cybersecurity requirement is
25 not necessary to secure the information

1 system or agency information stored on or
2 transiting it; and

3 “(iii) the agency has taken all nec-
4 essary steps to secure the information sys-
5 tem and agency information stored on or
6 transiting it; and

7 “(B) the head of the agency has submitted
8 the certification described in subparagraph (A)
9 to the appropriate congressional committees
10 and the authorizing committees of the agency.

11 “(4) DURATION OF CERTIFICATION.—

12 “(A) IN GENERAL.—A certification and
13 corresponding exemption of an agency under
14 paragraph (3) shall expire on the date that is
15 4 years after the date on which the head of the
16 agency submits the certification under para-
17 graph (3)(A).

18 “(B) RENEWAL.—Upon the expiration of a
19 certification of an agency under paragraph (3),
20 the head of the agency may submit an addi-
21 tional certification in accordance with that
22 paragraph.

23 “(5) RULES OF CONSTRUCTION.—Nothing in
24 this subsection shall be construed—

1 “(A) to alter the authority of the Sec-
2 retary, the Director, or the Director of the Na-
3 tional Institute of Standards and Technology in
4 implementing subchapter II of this title;

5 “(B) to affect the standards or process of
6 the National Institute of Standards and Tech-
7 nology;

8 “(C) to affect the requirement under sec-
9 tion 3553(a)(4); or

10 “(D) to discourage continued improve-
11 ments and advancements in the technology,
12 standards, policies, and guidelines used to pro-
13 mote Federal information security.

14 “(g) EXCEPTION.—

15 “(1) REQUIREMENTS.—The requirements under
16 subsection (f)(1) shall not apply to—

17 “(A) the Department of Defense;

18 “(B) a national security system; or

19 “(C) an element of the intelligence commu-
20 nity.

21 “(2) PROHIBITION.—The prohibition under
22 subsection (f)(2) shall not apply to—

23 “(A) internet of things devices that are or
24 comprise a national security system;

25 “(B) national security systems; or

1 “(C) a procured internet of things device
2 described in subsection (f)(2)(B) that the Chief
3 Information Officer of an agency determines
4 is—

5 “(i) necessary for research purposes;
6 or

7 “(ii) secured using alternative and ef-
8 fective methods appropriate to the function
9 of the internet of things device.”.

10 (b) REPORT ON EXEMPTIONS.—Section 3554(e)(1)
11 of title 44, United States Code, as amended by this Act,
12 is further amended—

13 (1) in subparagraph (C), by striking “and” at
14 the end;

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

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

18 “(E) with respect to any exemption from
19 the requirements of subsection (f)(3) that is ef-
20 fective on the date of submission of the report,
21 the number of information systems that have
22 received an exemption from those require-
23 ments.”.

24 (c) DURATION OF CERTIFICATION EFFECTIVE
25 DATE.—Paragraph (3) of section 3554(f) of title 44,

1 United States Code, as added by this Act, shall take effect
2 on the date that is 1 year after the date of enactment
3 of this Act.

4 (d) FEDERAL CYBERSECURITY ENHANCEMENT ACT
5 OF 2015 UPDATE.—Section 222(3)(B) of the Federal Cy-
6 bersecurity Enhancement Act of 2015 (6 U.S.C.
7 1521(3)(B)) is amended by inserting “and the Committee
8 on Oversight and Accountability” before “of the House of
9 Representatives.”

10 **SEC. 19. FEDERAL CHIEF INFORMATION SECURITY OFFI-**
11 **CER.**

12 (a) AMENDMENT.—Chapter 36 of title 44, United
13 States Code, is amended by adding at the end the fol-
14 lowing:

15 **“§ 3617. Federal Chief Information Security Officer**

16 “(a) ESTABLISHMENT.—There is established a Fed-
17 eral Chief Information Security Officer, who shall serve
18 in—

19 “(1) the Office of the Federal Chief Informa-
20 tion Officer of the Office of Management and Budg-
21 et; and

22 “(2) the Office of the National Cyber Director.

23 “(b) APPOINTMENT.—The Federal Chief Information
24 Security Officer shall be appointed by the President.

1 “(c) OMB DUTIES.—The Federal Chief Information
2 Security Officer shall report to the Federal Chief Informa-
3 tion Officer and assist the Federal Chief Information Offi-
4 cer in carrying out—

5 “(1) every function under this chapter;

6 “(2) every function assigned to the Director
7 under title II of the E-Government Act of 2002 (44
8 U.S.C. 3501 note; Public Law 107–347);

9 “(3) other electronic government initiatives con-
10 sistent with other statutes; and

11 “(4) other Federal cybersecurity initiatives de-
12 termined by the Federal Chief Information Officer.

13 “(d) ADDITIONAL DUTIES.—The Federal Chief In-
14 formation Security Officer shall—

15 “(1) support the Federal Chief Information Of-
16 ficer in overseeing and implementing Federal cyber-
17 security under the E-Government Act of 2002 (Pub-
18 lic Law 107–347; 116 Stat. 2899) and other rel-
19 evant statutes in a manner consistent with law; and

20 “(2) perform every function assigned to the Di-
21 rector under sections 1321 through 1328 of title 41,
22 United States Code.

23 “(e) COORDINATION WITH ONCD.—The Federal
24 Chief Information Security Officer shall support initiatives
25 determined by the Federal Chief Information Officer nec-

1 essary to coordinate with the Office of the National Cyber
2 Director.”.

3 (b) NATIONAL CYBER DIRECTOR DUTIES.—Section
4 1752 of the William M. (Mac) Thornberry National De-
5 fense Authorization Act for Fiscal Year 2021 (6 U.S.C.
6 1500) is amended—

7 (1) by redesignating subsection (g) as sub-
8 section (h); and

9 (2) by inserting after subsection (f) the fol-
10 lowing:

11 “(g) SENIOR FEDERAL CYBERSECURITY OFFICER.—
12 The Federal Chief Information Security Officer appointed
13 by the President under section 3617 of title 44, United
14 States Code, shall be a senior official within the Office
15 and carry out duties applicable to the protection of infor-
16 mation technology (as defined in section 11101 of title 40,
17 United States Code), including initiatives determined by
18 the Director necessary to coordinate with the Office of the
19 Federal Chief Information Officer.”.

20 (c) TREATMENT OF INCUMBENT.—The individual
21 serving as the Federal Chief Information Security Officer
22 appointed by the President as of the date of the enactment
23 of this Act may serve as the Federal Chief Information
24 Security Officer under section 3617 of title 44, United
25 States Code, as added by this Act, beginning on the date

1 of enactment of this Act, without need for a further or
2 additional appointment under such section.

3 (d) CLERICAL AMENDMENT.—The table of sections
4 for chapter 36 of title 44, United States Code, is amended
5 by adding at the end the following:

“Sec. 3617. Federal Chief Information Security Officer”.

6 **SEC. 20. RENAMING OFFICE OF THE FEDERAL CHIEF IN-**
7 **FORMATION OFFICER.**

8 (a) DEFINITIONS.—

9 (1) IN GENERAL.—Section 3601 of title 44,
10 United States Code, is amended—

11 (A) by striking paragraph (1); and

12 (B) by redesignating paragraphs (2)
13 through (8) as paragraphs (1) through (7), re-
14 spectively.

15 (2) CONFORMING AMENDMENTS.—

16 (A) TITLE 10.—Section 2222(i)(6) of title
17 10, United States Code, is amended by striking
18 “section 3601(4)” and inserting “section
19 3601”.

20 (B) NATIONAL SECURITY ACT OF 1947.—
21 Section 506D(k)(1) of the National Security
22 Act of 1947 (50 U.S.C. 3100(k)(1)) is amended
23 by striking “section 3601(4)” and inserting
24 “section 3601”.

1 (b) OFFICE OF ELECTRONIC GOVERNMENT.—Section
2 3602 of title 44, United States Code, is amended—

3 (1) in the heading, by striking “**OFFICE OF**
4 **ELECTRONIC GOVERNMENT**” and inserting “**OF-**
5 **FICE OF THE FEDERAL CHIEF INFORMATION**
6 **OFFICER**”;

7 (2) in subsection (a), by striking “Office of
8 Electronic Government” and inserting “Office of the
9 Federal Chief Information Officer”;

10 (3) in subsection (b), by striking “an Adminis-
11 trator” and inserting “a Federal Chief Information
12 Officer”;

13 (4) in subsection (c), in the matter preceding
14 paragraph (1), by striking “The Administrator” and
15 inserting “The Federal Chief Information Officer”;

16 (5) in subsection (d), in the matter preceding
17 paragraph (1), by striking “The Administrator” and
18 inserting “The Federal Chief Information Officer”;

19 (6) in subsection (e), in the matter preceding
20 paragraph (1), by striking “The Administrator” and
21 inserting “The Federal Chief Information Officer”;

22 (7) in subsection (f)—

23 (A) in the matter preceding paragraph (1),
24 by striking “the Administrator” and inserting
25 “the Federal Chief Information Officer”; and

1 (B) in paragraph (16), by striking “the
2 Office of Electronic Government” and inserting
3 “the Office of the Federal Chief Information
4 Officer”; and

5 (8) in subsection (g), by striking “the Office of
6 Electronic Government” and inserting “the Office of
7 the Federal Chief Information Officer”.

8 (c) CHIEF INFORMATION OFFICERS COUNCIL.—Sec-
9 tion 3603 of title 44, United States Code, is amended—

10 (1) in subsection (b)(2), by striking “The Ad-
11 ministrator of the Office of Electronic Government”
12 and inserting “The Federal Chief Information Offi-
13 cer”;

14 (2) in subsection (c)(1), by striking “The Ad-
15 ministrator of the Office of Electronic Government”
16 and inserting “The Federal Chief Information Offi-
17 cer”; and

18 (3) in subsection (f)—

19 (A) in paragraph (3), by striking “the Ad-
20 ministrator” and inserting “the Federal Chief
21 Information Officer”; and

22 (B) in paragraph (5), by striking “the Ad-
23 ministrator” and inserting “the Federal Chief
24 Information Officer”.

1 (d) E-GOVERNMENT FUND.—Section 3604 of title
2 44, United States Code, is amended—

3 (1) in subsection (a)(2), by striking “the Ad-
4 ministrator of the Office of Electronic Government”
5 and inserting “the Federal Chief Information Offi-
6 cer”;

7 (2) in subsection (b), by striking “Adminis-
8 trator” each place it appears and inserting “Federal
9 Chief Information Officer”; and

10 (3) in subsection (c), in the matter preceding
11 paragraph (1), by striking “the Administrator” and
12 inserting “the Federal Chief Information Officer”.

13 (e) PROGRAM TO ENCOURAGE INNOVATIVE SOLU-
14 TIONS TO ENHANCE ELECTRONIC GOVERNMENT SERV-
15 ICES AND PROCESSES.—Section 3605 of title 44, United
16 States Code, is amended—

17 (1) in subsection (a), by striking “The Adminis-
18 trator” and inserting “The Federal Chief Informa-
19 tion Officer”;

20 (2) in subsection (b), by striking “, the Admin-
21 istrator,” and inserting “, the Federal Chief Infor-
22 mation Officer,”; and

23 (3) in subsection (c)—

24 (A) in paragraph (1)—

1 (i) by striking “The Administrator”
2 and inserting “The Federal Chief Informa-
3 tion Officer”; and

4 (ii) by striking “proposals submitted
5 to the Administrator” and inserting “pro-
6 posals submitted to the Federal Chief In-
7 formation Officer”;

8 (B) in paragraph (2)(B), by striking “the
9 Administrator” and inserting “the Federal
10 Chief Information Officer”; and

11 (C) in paragraph (4), by striking “the Ad-
12 ministrator” and inserting “the Federal Chief
13 Information Officer”.

14 (f) E-GOVERNMENT REPORT.—Section 3606 of title
15 44, United States Code, is amended in the section heading
16 by striking “**E-Government**” and inserting “**An-**
17 **nual**”.

18 (g) TREATMENT OF INCUMBENT.—The individual
19 serving as the Administrator of the Office of Electronic
20 Government under section 3602 of title 44, United States
21 Code, as of the date of the enactment of this Act, may
22 continue to serve as the Federal Chief Information Officer
23 commencing as of that date, without need for a further
24 or additional appointment under such section.

1 (h) TECHNICAL AND CONFORMING AMENDMENTS.—
2 The table of sections for chapter 36 of title 44, United
3 States Code, is amended—

4 (1) by striking the item relating to section 3602
5 and inserting the following:

“3602. Office of the Federal Chief Information Officer.”;

6 and

7 (2) in the item relating to section 3606, by
8 striking “E-Government” and inserting “Annual”.

9 (i) REFERENCES.—

10 (1) ADMINISTRATOR.—Any reference to the Ad-
11 ministrator of the Office of Electronic Government
12 in any law, regulation, map, document, record, or
13 other paper of the United States shall be deemed to
14 be a reference to the Federal Chief Information Offi-
15 cer.

16 (2) OFFICE OF ELECTRONIC GOVERNMENT.—
17 Any reference to the Office of Electronic Govern-
18 ment in any law, regulation, map, document, record,
19 or other paper of the United States shall be deemed
20 to be a reference to the Office of the Federal Chief
21 Information Officer.

22 **SEC. 21. RULES OF CONSTRUCTION.**

23 (a) AGENCY ACTIONS.—Nothing in this Act, or an
24 amendment made by this Act, shall be construed to au-
25 thorize the head of an agency to take an action that is

1 not authorized by this Act, an amendment made by this
2 Act, or existing law.

3 (b) PROTECTION OF RIGHTS.—Nothing in this Act,
4 or an amendment made by this Act, shall be construed
5 to permit the violation of the rights of any individual pro-
6 tected by the Constitution of the United States, including
7 through censorship of speech protected by the Constitu-
8 tion of the United States or unauthorized surveillance.

○