

**AMENDMENT IN THE NATURE OF A SUBSTITUTE
TO H.R. 4552
OFFERED BY MR. COMER OF KENTUCKY**

Strike all after the enacting clause and insert the following:

1 SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

2 (a) SHORT TITLE.—This Act may be cited as the
3 “Federal Information Security Modernization Act of
4 2024”.

5 (b) TABLE OF CONTENTS.—The table of contents for
6 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. Agency requirements to notify private sector entities impacted by incidents.
- Sec. 7. Federal penetration testing policy.
- Sec. 8. Vulnerability disclosure policies.
- Sec. 9. Implementing zero trust architecture.
- Sec. 10. Automation and artificial intelligence.
- Sec. 11. Federal cybersecurity requirements.
- Sec. 12. Federal Chief Information Security Officer.
- Sec. 13. Renaming Office of the Federal Chief Information Officer.
- Sec. 14. Rules of construction.

7 SEC. 2. DEFINITIONS.

8 In this Act, unless otherwise specified:

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

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

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

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

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

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

14 (4) CONTRACTOR.—The term “contractor” has
15 the meaning given the term in section 3591 of title
16 44, United States Code, as added by this Act.

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

20 (6) FEDERAL INFORMATION SYSTEM.—The
21 term “Federal information system” has the meaning
22 given the term in section 3591 of title 44, United
23 States Code, as added by this Act.

1 (7) INCIDENT.—The term “incident” has the
2 meaning given the term in section 3552(b) of title
3 44, United States Code.

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

8 (9) PENETRATION TEST.—The term “penetra-
9 tion test” has the meaning given the term in section
10 3552(b) of title 44, United States Code, as amended
11 by this Act.

12 (10) THREAT HUNTING.—The term “threat
13 hunting” means proactively and iteratively searching
14 systems for threats and vulnerabilities, including
15 threats or vulnerabilities that may evade detection
16 by automated threat detection systems.

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

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

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

25 (1) in section 3504—

1 (A) in subsection (a)(1)(B)—

2 (i) by striking clause (v) and inserting
3 the following:

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

6 (ii) by redesignating clause (vi) as
7 clause (vii); and

8 (iii) by inserting after clause (v) the
9 following:

10 “(vi) in consultation with the National
11 Cyber Director, security of information;
12 and”; and

13 (B) in subsection (g)—

14 (i) by redesignating paragraph (2) as
15 paragraph (3); and

16 (ii) by striking paragraph (1) and in-
17 sserting the following:

18 “(1) develop and oversee the implementation of
19 policies, principles, standards, and guidelines on pri-
20 vacy, confidentiality, disclosure, and sharing of in-
21 formation collected or maintained by or for agencies;

22 “(2) in consultation with the National Cyber
23 Director, oversee the implementation of policies,
24 principles, standards, and guidelines on security, of

1 information collected or maintained by or for agen-
2 cies; and”;

3 (2) in section 3505—

4 (A) by striking the first subsection des-
5 igned as subsection (c);

6 (B) in paragraph (2) of the second sub-
7 section designated as subsection (c), by insert-
8 ing “an identification of internet accessible in-
9 formation systems and” after “an inventory
10 under this subsection shall include”;

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

13 (i) in subparagraph (B)—

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

19 (II) by striking “and” at the end;

20 (ii) in subparagraph (C)(v), by strik-
21 ing the period at the end and inserting “;
22 and”; and

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

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

5 (A) in subsection (a)(3), by inserting “In
6 carrying out these duties, the Chief Information
7 Officer shall consult, as appropriate, with the
8 Chief Data Officer in accordance with the des-
9 ignated functions under section 3520(c).” after
10 “reduction of information collection burdens on
11 the public.”;

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

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

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

17 “(j)(1) Notwithstanding paragraphs (2) and (3) of
18 subsection (a), the head of each agency shall, in accord-
19 ance with section 522(a) of division H of the Consolidated
20 Appropriations Act, 2005 (42 U.S.C. 2000ee–2), des-
21 ignate a Chief Privacy Officer with the necessary skills,
22 knowledge, and expertise, who shall have the authority and
23 responsibility to—

24 “(A) lead the privacy program of the agency;

25 and

1 “(B) carry out the privacy responsibilities of
2 the agency under this chapter, section 552a of title
3 5, and guidance issued by the Director.

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

5 “(A) serve in a central leadership position with-
6 in the agency;

7 “(B) have visibility into relevant agency oper-
8 ations; and

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

12 “(3) A privacy officer of an agency established under
13 a statute enacted before the date of enactment of the Fed-
14 eral Information Security Modernization Act of 2024 may
15 carry out the responsibilities under this subsection for the
16 agency.”; and

17 (4) in section 3513—

18 (A) by redesignating subsection (c) as sub-
19 section (d); and

20 (B) by inserting after subsection (b) the
21 following:

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

1 (b) SUBCHAPTER II DEFINITIONS.—

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

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

7 (B) by inserting after paragraph (1) the
8 following:

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

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

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

24 (D) in paragraph (8)(A), as so redesign-
25 nated, in the matter preceding clause (i), by

1 striking “used” and inserting “owned, man-
2 aged,”;

3 (E) by inserting after paragraph (8), as so
4 redesignated, the following:

5 “(9) The term ‘penetration test’—

6 “(A) means an authorized assessment that
7 emulates attempts to gain unauthorized access
8 to, or disrupt the operations of, an information
9 system or component of an information system;
10 and

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

15 (F) by inserting after paragraph (10), as
16 so redesignated, the following:

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

21 “(12) The term ‘zero trust architecture’ has the
22 meaning given the term in Special Publication 800-
23 207 of the National Institute of Standards and
24 Technology, or any successor document.”.

25 (2) CONFORMING AMENDMENTS.—

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

6 (B) TITLE 10.—

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

11 (ii) SECTION 2223.—Section
12 2223(c)(3) of title 10, United States Code,
13 is amended by striking “section
14 3552(b)(6)” and inserting “section
15 3552(b)”.

16 (iii) SECTION 3068.—Section 3068(b)
17 of title 10, United States Code, is amended
18 by striking “section 3552(b)(6)” and in-
19 serting “section 3552(b)”.

20 (iv) SECTION 3252.—Section
21 3252(e)(5) of title 10, United States Code,
22 is amended by striking “section
23 3552(b)(6)” and inserting “section
24 3552(b)”.

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

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

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

19 (F) IKE SKELTON NATIONAL DEFENSE AU-
20 THORIZATION ACT FOR FISCAL YEAR 2011.—The
21 Ike Skelton National Defense Authorization Act
22 for Fiscal Year 2011 (Public Law 111–383) is
23 amended—

1 (i) in section 806(e)(5) (10 U.S.C.
2 2304 note), by striking “section 3542(b)”
3 and inserting “section 3552(b)”;

4 (ii) in section 931(b)(3) (10 U.S.C.
5 2223 note), by striking “section
6 3542(b)(2)” and inserting “section
7 3552(b)”;

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

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

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

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

24 (ii) in subsection (f)—

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

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

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

10 (1) in section 3551—

11 (A) in paragraph (4), by striking “diag-
12 nose and improve” and inserting “integrate, de-
13 liver, diagnose, and improve”;

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

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

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

19 “(7) recognize that each agency has specific
20 mission requirements and, at times, unique cyberse-
21 curity requirements to meet the mission of the agen-
22 cy;

23 “(8) recognize that each agency does not have
24 the same resources to secure agency systems, and an
25 agency should not be expected to have the capability

1 to secure the systems of the agency from advanced
2 adversaries alone; and

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

6 (2) in section 3553—

7 (A) in subsection (a)—

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

10 (ii) in paragraph (6), by striking the
11 period at the end and inserting “; and”;

12 and

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

15 “(7) promoting, in consultation with the Direc-
16 tor of the Cybersecurity and Infrastructure Security
17 Agency, the National Cyber Director, and the Direc-
18 tor of the National Institute of Standards and Tech-
19 nology—

20 “(A) the use of automation to improve
21 Federal cybersecurity and visibility with respect
22 to the implementation of Federal cybersecurity;
23 and

24 “(B) the use of presumption of com-
25 promise and least privilege principles, such as

1 zero trust architecture, to improve resiliency
2 and timely response actions to incidents on
3 Federal systems.”;

4 (B) in subsection (b)—

5 (i) in the matter preceding paragraph
6 (1), by inserting “and the National Cyber
7 Director” after “Director”;

8 (ii) in paragraph (2)(A), by inserting
9 “and reporting requirements under sub-
10 chapter IV of this chapter” after “section
11 3556”;

12 (iii) by redesignating paragraphs (8)
13 and (9) as paragraphs (10) and (11), re-
14 spectively; and

15 (iv) by inserting after paragraph (7)
16 the following:

17 “(8) expeditiously seeking opportunities to re-
18 duce costs, administrative burdens, and other bar-
19 riers to information technology security and mod-
20 ernization for agencies, including through shared
21 services (and appropriate commercial off the shelf
22 options for such shared services) for cybersecurity
23 capabilities identified as appropriate by the Director,
24 in coordination with the Director of the Cybersecu-

1 rity and Infrastructure Security Agency and other
2 agencies as appropriate;”;

3 (C) in subsection (c)—

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

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

10 (II) by inserting “, which shall be
11 unclassified but may include 1 or
12 more annexes that contain classified
13 or other sensitive information, as ap-
14 propriate” after “a report”; and

15 (III) by striking “preceding
16 year” and inserting “preceding 2
17 years”;

18 (ii) by striking paragraph (1);

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

22 (iv) in paragraph (3), as so redesign-
23 dated, by striking “and” at the end; and

24 (v) by inserting after paragraph (3),
25 as so redesignated, the following:

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

4 (D) in subsection (h)—

5 (i) in paragraph (2)—

6 (I) in subparagraph (A), by in-
7 serting “and the National Cyber Di-
8 rector” after “in coordination with the
9 Director”;

10 (II) in subparagraph (B), by in-
11 serting “, the scope of the required
12 action (such as applicable software,
13 firmware, or hardware versions),”
14 after “reasons for the required ac-
15 tion”; and

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

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

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

1 “(i) FEDERAL RISK ASSESSMENT.—On an ongoing
2 and continual basis, the Director of the Cybersecurity and
3 Infrastructure Security Agency shall assess the Federal
4 risk posture using any available information on the cyber-
5 security posture of agencies, and brief the Director and
6 National Cyber Director on the findings of such assess-
7 ment, 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 the results of the review
14 under paragraph (1).

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

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

1 consider developing and, if appropriate and practical, de-
2 velop specifications to enable the automated verification
3 of the implementation of the controls.

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

11 (3) in section 3554—

12 (A) in subsection (a)—

13 (i) in paragraph (1)—

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

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

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

23 “(i) identifying and documenting the
24 high value assets of the agency using guid-
25 ance from the Director;

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

5 “(iii) identifying whether the agency
6 is participating in federally offered cyber-
7 security shared services programs;

8 “(iv) identifying agency systems that
9 have access to or hold the data assets
10 inventoried under section 3511;

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

16 “(vi) evaluating the vulnerability of
17 agency systems and data, including high
18 value assets, including by analyzing—

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

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

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

5 “(IV) incidents; and

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

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

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

23 (III) in subparagraph (B), as so
24 redesignated, in the matter preceding
25 clause (i), by striking “providing in-

1 formation” and inserting “using infor-
2 mation from the assessment required
3 under subparagraph (A), providing in-
4 formation”;

5 (IV) in subparagraph (C), as so
6 redesignated—

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

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

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

14 “(E) providing an update on the ongoing
15 and continual assessment required under sub-
16 paragraph (A)—

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

20 “(ii) at intervals determined by guid-
21 ance issued by the Director, and to the ex-
22 tent appropriate and practicable using au-
23 tomation, to—

24 “(I) the Director;

1 “(II) the Director of the Cyberse-
2 curity and Infrastructure Security
3 Agency; and

4 “(III) the National Cyber Direc-
5 tor;”;

6 (ii) in paragraph (2)—

7 (I) in subparagraph (A), by in-
8 serting “in accordance with the agen-
9 cy system risk assessment required
10 under paragraph (1)(A)” after “infor-
11 mation systems”; and

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

18 (iii) in paragraph (3)(A)—

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

23 (II) in clause (i), by striking
24 “this section” and inserting “sub-
25 sections (a) through (c)”;

1 (III) in clause (ii), by striking
2 “training and” and inserting “skills,
3 training, and”;

4 (IV) by redesignating clauses (iii)
5 and (iv) as (iv) and (v), respectively;

6 (V) by inserting after clause (ii)
7 the following:

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

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

20 (iv) in paragraph (5), by striking “an-
21 nually” and inserting “not less frequently
22 than quarterly”; and

23 (v) in paragraph (6), by striking “offi-
24 cial delegated” and inserting “Chief Infor-
25 mation Security Officer delegated”;

1 (B) in subsection (b)—

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

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

10 (ii) in paragraph (2)—

11 (I) by striking subparagraph (B);

12 (II) by redesignating subpara-
13 graphs (C) and (D) as subparagraphs
14 (B) and (C), respectively;

15 (III) in subparagraph (B), as so
16 redesignated, by striking “and” at the
17 end; and

18 (IV) in subparagraph (C), as so
19 redesignated—

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

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

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

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

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

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

17 (v) by inserting after paragraph (6)
18 the following:

19 “(7) a process for securely providing the status
20 of remedial cybersecurity actions and un-remediated
21 identified system vulnerabilities of high value assets
22 to the Director and the Director of the Cybersecu-
23 rity and Infrastructure Security Agency, using auto-
24 mation and machine-readable data as appropriate;”;
25 and

1 (vi) in paragraph (8)(C), as so redese-
2 gnated—

3 (I) by striking clause (ii) and in-
4 serting the following:

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

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

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

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

16 (IV) in clause (iv), as so redese-
17 gnated—

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

20 (bb) by striking subclause
21 (III); and

22 (cc) by redesignating sub-
23 clause (IV) as subclause (III);

24 and

25 (C) in subsection (c)—

1 (i) by redesignating paragraph (2) as
2 paragraph (4);

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

5 “(1) BIENNIAL REPORT.—Not later than 2
6 years after the date of enactment of the Federal In-
7 formation Security Modernization Act of 2024 and
8 not less frequently than once every 2 years there-
9 after, using the ongoing and continual agency sys-
10 tem risk assessment required under subsection
11 (a)(1)(A), the head of each agency shall submit to
12 the Director, the National Cyber Director, the Di-
13 rector of the Cybersecurity and Infrastructure Secu-
14 rity Agency, the Comptroller General of the United
15 States, the majority and minority leaders of the Sen-
16 ate, the Speaker and minority leader of the House
17 of Representatives, the Committee on Homeland Se-
18 curity and Governmental Affairs of the Senate, the
19 Committee on Oversight and Accountability of the
20 House of Representatives, the Committee on Home-
21 land Security of the House of Representatives, the
22 Committee on Commerce, Science, and Transpor-
23 tation of the Senate, the Committee on Science,
24 Space, and Technology of the House of Representa-

1 tives, and the appropriate authorization and appro-
2 priations committees of Congress a report that—

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

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

14 “(C) summarizes the status of remedial ac-
15 tions identified by inspector general of the
16 agency, the Comptroller General of the United
17 States, and any other source determined appro-
18 priate by the head of the agency; and

19 “(D) includes the cybersecurity shared
20 services offered by the Cybersecurity and Infra-
21 structure Security Agency that the agency par-
22 ticipates in, if any, and explanations for any
23 non-participation in such services.

24 “(2) UNCLASSIFIED REPORTS.—Each report
25 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 (4), 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 (F) by striking subsection (j) and inserting
6 the following:

7 “(j) GUIDANCE.—

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

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

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

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

24 “(C) any other security risks unique to
25 Federal systems; and

1 “(D) any other element the Director deter-
2 mines appropriate.”; and

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

4 “(k) COORDINATION.—The head of each agency shall
5 coordinate with the inspector general of the agency, as ap-
6 plicable, to ensure consistent understanding of agency cy-
7 bersecurity or information security policies for the purpose
8 of evaluations of such policies conducted by the inspector
9 general.”; and

10 (5) in section 3556(a)—

11 (A) in the matter preceding paragraph (1),
12 by inserting “within the Cybersecurity and In-
13 frastructure Security Agency” after “incident
14 center”; and

15 (B) in paragraph (4), by striking
16 “3554(b)” and inserting “3554(a)(1)(A)”.

17 (d) CONFORMING AMENDMENTS.—

18 (1) TABLE OF SECTIONS.—The table of sections
19 for chapter 35 of title 44, United States Code, is
20 amended by striking the item relating to section
21 3555 and inserting the following:

 “3555. Independent evaluation.”.

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

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

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

9 (i) by striking “annually thereafter”
10 and inserting “thereafter during the years
11 during which a report is required to be
12 submitted under section 3553(c) of title
13 44, United States Code”; and

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

17 (3) NIST RESPONSIBILITIES.—Section
18 20(d)(3)(B) of the National Institute of Standards
19 and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is
20 amended by striking “annual”.

21 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

1 “SUBCHAPTER IV—FEDERAL SYSTEM
2 INCIDENT RESPONSE

3 **“§ 3591. Definitions**

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

7 “(b) ADDITIONAL DEFINITIONS.—As used in this
8 subchapter:

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

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

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

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

17 “(D) the Committee on Commerce,
18 Science, and Transportation of the Senate;

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

21 “(F) the Committee on Homeland Security
22 of the House of Representatives;

23 “(G) the Committee on Science, Space,
24 and Technology of the House of Representa-
25 tives;

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

3 “(I) the Director;

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

6 “(K) the National Cyber Director;

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

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

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

13 “(A) means—

14 “(i) the recipient of a grant from an
15 agency;

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

18 “(iii) a party to an other transaction
19 agreement with an agency; and

20 “(B) includes a subawardee of an entity
21 described in subparagraph (A).

22 “(3) BREACH.—The term ‘breach’—

23 “(A) means the compromise, unauthorized
24 disclosure, unauthorized acquisition, or loss of
25 control of personally identifiable information

1 owned, maintained or otherwise controlled by
2 an agency, or any similar occurrence; and

3 “(B) includes any additional meaning
4 given the term in policies, principles, standards,
5 or guidelines issued by the Director.

6 “(4) CONTRACTOR.—The term ‘contractor’
7 means a prime contractor of an agency or a subcon-
8 tractor of a prime contractor of an agency that cre-
9 ates, collects, stores, processes, maintains, or trans-
10 mits Federal information on behalf of an agency.

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

16 “(6) FEDERAL INFORMATION SYSTEM.—The
17 term ‘Federal information system’ means an infor-
18 mation system owned, managed, or operated by an
19 agency, or on behalf of an agency by a contractor,
20 an awardee, or another organization.

21 “(7) INTELLIGENCE COMMUNITY.—The term
22 ‘intelligence community’ has the meaning given the
23 term in section 3 of the National Security Act of
24 1947 (50 U.S.C. 3003).

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

6 “(9) VULNERABILITY DISCLOSURE.—The term
7 ‘vulnerability disclosure’ means a vulnerability iden-
8 tified under section 3559B.

9 **“§ 3592. Notification of breach**

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

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

14 “(2) the result of which the head of an agency
15 determines that notifying potentially affected indi-
16 viduals is necessary pursuant to subsection (b)(1),
17 regardless of whether—

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

20 “(B) the notification is delayed under sub-
21 section (d).

22 “(b) NOTIFICATION.—As expeditiously as practicable
23 and without unreasonable delay, and in any case not later
24 than 45 days after an agency has a reasonable basis to
25 conclude that a breach has occurred, the head of the agen-

1 cy, in consultation with the Chief Information Officer and
2 Chief Privacy Officer of the agency and, as appropriate,
3 any non-Federal entity supporting the remediation of the
4 breach, shall—

5 “(1) determine whether notice to any individual
6 potentially affected by the breach is appropriate, in-
7 cluding by conducting an assessment of the risk of
8 harm to the individual that considers—

9 “(A) the nature and sensitivity of the per-
10 sonally identifiable information affected by the
11 breach;

12 “(B) the likelihood of access to and use of
13 the personally identifiable information affected
14 by the breach;

15 “(C) the type of breach; and

16 “(D) any other factors determined by the
17 Director; and

18 “(2) if the head of the agency determines notifi-
19 cation is necessary pursuant to paragraph (1), pro-
20 vide written notification in accordance with sub-
21 section (c) to each individual potentially affected by
22 the breach—

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

1 “(B) through an appropriate alternative
2 method of notification.

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

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

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

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

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

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

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

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

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

4 “(d) DELAY OF NOTIFICATION.—

5 “(1) IN GENERAL.—The head of an agency, in
6 coordination with the Director and the National
7 Cyber Director, and as appropriate, the Attorney
8 General, the Director of National Intelligence, or the
9 Secretary of Homeland Security, may delay a notifi-
10 cation required under subsection (b) or (e) if the no-
11 tification would—

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

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

16 “(C) reveal sensitive sources and methods;

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

18 “(E) hamper security remediation actions.

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

21 “(3) NATIONAL SECURITY SYSTEMS.—The head
22 of an agency delaying notification under this sub-
23 section with respect to a breach exclusively of a na-
24 tional security system shall coordinate such delay
25 with the Secretary of Defense.

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

12 “(f) DELAY OF NOTIFICATION REPORT.—

13 “(1) IN GENERAL.—Not later than 1 year after
14 the date of enactment of the Federal Information
15 Security Modernization Act of 2024, and annually
16 thereafter, the head of an agency, in coordination
17 with any official who delays a notification under sub-
18 section (d), shall submit to the appropriate reporting
19 entities a report on each delay that occurred during
20 the previous 2 years.

21 “(2) COMPONENT OF OTHER REPORT.—The
22 head of an agency may submit the report required
23 under paragraph (1) as a component of the report
24 submitted under section 3554(c).

1 “(g) CONGRESSIONAL REPORTING REQUIRE-
2 MENTS.—

3 “(1) REVIEW AND UPDATE.—On a periodic
4 basis, the Director of the Office of Management and
5 Budget shall review, and update as appropriate,
6 breach notification policies and guidelines for agen-
7 cies.

8 “(2) REQUIRED NOTICE FROM AGENCIES.—
9 Subject to paragraph (4), the Director of the Office
10 of Management and Budget shall require the head
11 of an agency affected by a covered breach to expedi-
12 tiously and not later than 30 days after the date on
13 which the agency discovers the covered breach give
14 notice of the breach, which may be provided elec-
15 tronically, to—

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

18 “(B) the Committee on the Judiciary of
19 the Senate and the Committee on the Judiciary
20 of the House of Representatives.

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

1 “(A) information about the covered breach,
2 including a summary of any information about
3 how the covered breach occurred known by the
4 agency as of the date of the notice;

5 “(B) an estimate of the number of individ-
6 uals affected by the covered breach based on in-
7 formation known by the agency as of the date
8 of the notice, including an assessment of the
9 risk of harm to affected individuals;

10 “(C) a description of any circumstances
11 necessitating a delay in providing notice to indi-
12 viduals affected by the covered breach in ac-
13 cordance with subsection (d); and

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

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

21 “(A) the majority and minority leaders of
22 the Senate;

23 “(B) the Speaker and minority leader of
24 the House of Representatives;

1 “(C) the appropriations committees of
2 Congress;

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

5 “(E) the Select Committee on Intelligence
6 of the Senate;

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

10 “(G) the Permanent Select Committee on
11 Intelligence of the House of Representatives.

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

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

17 “(1) limit—

18 “(A) the authority of the Director to issue
19 guidance relating to notifications of, or the
20 head of an agency to notify individuals poten-
21 tially affected by, breaches that are not deter-
22 mined to be covered breaches or major inci-
23 dents;

24 “(B) the authority of the Director to issue
25 guidance relating to notifications and reporting

1 of breaches, covered breaches, or major inci-
2 dents;

3 “(C) the authority of the head of an agen-
4 cy to provide more information than required
5 under subsection (b) when notifying individuals
6 potentially affected by a breach;

7 “(D) the timing of incident reporting or
8 the types of information included in incident re-
9 ports provided, pursuant to this subchapter,
10 to—

11 “(i) the Director;

12 “(ii) the National Cyber Director;

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

15 “(iv) any other agency;

16 “(E) the authority of the head of an agen-
17 cy to provide information to Congress about
18 agency breaches, including—

19 “(i) breaches that are not covered
20 breaches; and

21 “(ii) additional information beyond
22 the information described in subsection
23 (g)(3); or

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

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

3 **“§ 3593. Congressional and executive branch reports**
4 **on major incidents**

5 “(a) APPROPRIATE CONGRESSIONAL ENTITIES.—In
6 this section, the term ‘appropriate congressional entities’
7 means—

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

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

12 “(3) the Committee on Homeland Security and
13 Governmental Affairs of the Senate;

14 “(4) the Committee on Commerce, Science, and
15 Transportation of the Senate;

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

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

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

22 “(8) the appropriate authorization and appro-
23 priations committees of Congress.

24 “(b) INITIAL NOTIFICATION.—

1 “(1) IN GENERAL.—Not later than 72 hours
2 after an agency has a reasonable basis to conclude
3 that a major incident occurred, the head of the
4 agency impacted by the major incident shall submit
5 to the appropriate reporting entities a written notifi-
6 cation, which may be submitted electronically and
7 include 1 or more annexes that contain classified or
8 other sensitive information, as appropriate.

9 “(2) CONTENTS.—A notification required under
10 paragraph (1) with respect to a major incident shall
11 include the following, based on information available
12 to agency officials as of the date on which the agen-
13 cy submits the notification:

14 “(A) A summary of the information avail-
15 able about the major incident, including how
16 the major incident occurred and the threat
17 causing the major incident.

18 “(B) If applicable, information relating to
19 any breach associated with the major incident,
20 regardless of whether—

21 “(i) the breach was the reason the in-
22 cident was determined to be a major inci-
23 dent; and

24 “(ii) head of the agency determined it
25 was appropriate to provide notification to

1 potentially impacted individuals pursuant
2 to section 3592(b)(1).

3 “(C) A preliminary assessment of the im-
4 pacts to—

5 “(i) the agency;

6 “(ii) the Federal Government;

7 “(iii) the national security, foreign re-
8 lations, homeland security, and economic
9 security of the United States; and

10 “(iv) the civil liberties, public con-
11 fidence, privacy, and public health and
12 safety of the people of the United States.

13 “(D) If applicable, whether any ransom
14 has been demanded or paid, or is expected to be
15 paid, by any entity operating a Federal infor-
16 mation system or with access to Federal infor-
17 mation or a Federal information system, includ-
18 ing, as available, the name of the entity de-
19 manding ransom, the date of the demand, and
20 the amount and type of currency demanded, un-
21 less disclosure of such information will disrupt
22 an active Federal law enforcement or national
23 security operation.

24 “(c) SUPPLEMENTAL UPDATE.—Within a reasonable
25 amount of time, but not later than 30 days after the date

1 on which the head of an agency submits a written notifica-
2 tion under subsection (b), the head of the agency shall
3 provide to the appropriate congressional entities an un-
4 classified and written update, which may include 1 or
5 more annexes that contain classified or other sensitive in-
6 formation, as appropriate, on the major incident, based
7 on information available to agency officials as of the date
8 on which the agency provides the update, on—

9 “(1) system vulnerabilities relating to the major
10 incident, where applicable, means by which the
11 major incident occurred, the threat causing the
12 major incident, where applicable, and impacts of the
13 major incident to—

14 “(A) the agency;

15 “(B) other Federal agencies, Congress, or
16 the judicial branch;

17 “(C) the national security, foreign rela-
18 tions, homeland security, or economic security
19 of the United States; or

20 “(D) the civil liberties, public confidence,
21 privacy, or public health and safety of the peo-
22 ple of the United States;

23 “(2) the status of compliance of the affected
24 Federal information system with applicable security
25 requirements at the time of the major incident;

1 “(3) if the major incident involved a breach, a
2 description of the affected information, an estimate
3 of the number of individuals potentially impacted,
4 and any assessment to the risk of harm to such indi-
5 viduals;

6 “(4) an update to the assessment of the risk to
7 agency operations, or to impacts on other agency or
8 non-Federal entity operations, affected by the major
9 incident;

10 “(5) the detection, response, and remediation
11 actions of the agency, including any support pro-
12 vided by the Cybersecurity and Infrastructure Secu-
13 rity Agency under section 3594(d), if applicable;

14 “(6) as appropriate and available, actions un-
15 dertaken by any non-Federal entities impacted by or
16 supporting remediation of the major incident; and

17 “(7) as appropriate and available, recommenda-
18 tions for mitigating future similar incidents, includ-
19 ing recommendations from any non-Federal entity
20 impacted by or supporting the remediation of the
21 major incident.

22 “(d) ADDITIONAL UPDATE.—If the head of an agen-
23 cy, the Director, or the National Cyber Director deter-
24 mines that there is any significant change in the under-
25 standing of the scope, scale, or consequence of a major

1 incident for which the head of the agency submitted a
2 written notification and update under subsections (b) and
3 (c), the head of the agency shall submit to the appropriate
4 congressional entities a written update that includes infor-
5 mation relating to the change in understanding.

6 “(e) BIENNIAL REPORT.—Each agency shall submit
7 as part of the biennial report required under section
8 3554(c)(1) a description of each major incident that oc-
9 curred during the 2-year period preceding the date on
10 which the biennial report is submitted.

11 “(f) REPORT DELIVERY.—

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

14 “(A) shall be submitted in an electronic
15 format; and

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

17 “(2) CLASSIFICATION STATUS.—Any written
18 notification or update required to be submitted
19 under this section—

20 “(A) shall be—

21 “(i) unclassified; and

22 “(ii) submitted through unclassified
23 electronic means pursuant to paragraph
24 (1)(A); and

1 “(B) may include classified annexes, as ap-
2 propriate.

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

6 “(1) provide recommendations to agencies on
7 formatting and the contents of information to be in-
8 cluded in the reports required under this section, in-
9 cluding recommendations for consistent formats for
10 presenting any associated metrics; and

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

14 “(A) include, at a minimum—

15 “(i) the full contents of the written
16 notification or update;

17 “(ii) the identity of the reporting
18 agency; and

19 “(iii) the date of submission; and

20 “(iv) a list of the recipient congres-
21 sional entities; and

22 “(B) be made available upon request to the
23 majority and minority leaders of the Senate, the
24 Speaker and minority leader of the House of
25 Representatives, the Committee on Homeland

1 Security and Governmental Affairs of the Sen-
2 ate, and the Committee on Oversight and Ac-
3 countability of the House of Representatives.

4 “(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL
5 REPORTING EXEMPTION.—With respect to a major inci-
6 dent that occurs exclusively on a national security system,
7 the head of the affected agency shall submit the notifica-
8 tions and reports required to be submitted to Congress
9 under this section only to—

10 “(1) the majority and minority leaders of the
11 Senate;

12 “(2) the Speaker and minority leader of the
13 House of Representatives;

14 “(3) the appropriations committees of Con-
15 gress;

16 “(4) the appropriate authorization committees
17 of Congress;

18 “(5) the Committee on Homeland Security and
19 Governmental Affairs of the Senate;

20 “(6) the Select Committee on Intelligence of the
21 Senate;

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

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

1 “(i) MAJOR INCIDENTS INCLUDING BREACHES.—If
2 a major incident constitutes a covered breach, as defined
3 in section 3592(a), information on the covered breach re-
4 quired to be submitted to Congress pursuant to section
5 3592(g) may—

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

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

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

12 “(1) limit—

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

15 “(B) Congress from requesting additional
16 information from agencies through reports,
17 briefings, or other means;

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

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

22 **“§ 3594. Government information sharing and inci-**
23 **dent response**

24 “(a) IN GENERAL.—

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

11 “(2) CONTENTS.—A provision of information
12 relating to an incident made by the head of an agen-
13 cy under paragraph (1) shall include, at a min-
14 imum—

15 “(A) a full description of the incident, in-
16 cluding—

17 “(i) all indicators of compromise and
18 tactics, techniques, and procedures;

19 “(ii) an indicator of how the intruder
20 gained initial access, accessed agency data
21 or systems, and undertook additional ac-
22 tions on the network of the agency;

23 “(iii) information that would support
24 enabling defensive measures; and

1 “(iv) other information that may as-
2 sist in identifying other victims;

3 “(B) information to help prevent similar
4 incidents, such as information about relevant
5 safeguards in place when the incident occurred
6 and the effectiveness of those safeguards; and

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

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

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

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

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

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

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

1 “(i) the head of any agency that may
2 be—

3 “(I) impacted by the incident;

4 “(II) particularly susceptible to
5 the incident; or

6 “(III) similarly targeted by the
7 incident; and

8 “(ii) appropriate Federal law enforce-
9 ment agencies to facilitate any necessary
10 threat response activities, as requested;

11 “(C) coordinate any necessary information
12 sharing efforts relating to a major incident with
13 the private sector; and

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

16 “(4) NATIONAL SECURITY SYSTEMS EXEMP-
17 TION.—

18 “(A) IN GENERAL.—Notwithstanding
19 paragraphs (1) and (3), each agency operating
20 or exercising control of a national security sys-
21 tem shall share information about an incident
22 that occurs exclusively on a national security
23 system with the Secretary of Defense, the Di-
24 rector, the National Cyber Director, and the
25 Director of the Cybersecurity and Infrastruc-

1 ture Security Agency to the extent consistent
2 with standards and guidelines for national secu-
3 rity systems issued in accordance with law and
4 as directed by the President.

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

15 “(b) AUTOMATION.—In providing information and
16 selecting a method to provide information under sub-
17 section (a), the head of each agency shall implement sub-
18 section (a)(1) in a manner that provides such information
19 to the Cybersecurity and Infrastructure Security Agency
20 in an automated and machine-readable format, to the
21 greatest extent practicable.

22 “(c) INCIDENT RESPONSE.—Each agency that has a
23 reasonable basis to suspect or conclude that a major inci-
24 dent occurred involving Federal information in electronic

1 medium or form that does not exclusively involve a na-
2 tional security system shall coordinate with—

3 “(1) the Cybersecurity and Infrastructure Secu-
4 rity Agency to facilitate asset response activities and
5 provide recommendations for mitigating future inci-
6 dents; and

7 “(2) consistent with relevant policies, appro-
8 priate Federal law enforcement agencies to facilitate
9 threat response activities.

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

11 “(a) NOTIFICATION.—

12 “(1) IN GENERAL.—Any contractor or awardee
13 of an agency shall provide written notification to the
14 agency if the contractor or awardee has a reasonable
15 basis to conclude that—

16 “(A) an incident or breach has occurred
17 with respect to Federal information the con-
18 tractor or awardee collected, used, or main-
19 tained on behalf of an agency;

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

24 “(C) a component of any Federal informa-
25 tion system operated, managed, or maintained

1 by a contractor or awardee contains a security
2 vulnerability, including a supply chain com-
3 promise or an identified software or hardware
4 vulnerability, for which there is reliable evidence
5 of a successful exploitation of the vulnerability
6 by an actor without authorization of the Fed-
7 eral information system owner; or

8 “(D) the contractor or awardee has re-
9 ceived from the agency personally identifiable
10 information or personal health information that
11 is beyond the scope of the contract or agree-
12 ment with the agency that the contractor or
13 awardee is not authorized to receive.

14 “(2) THIRD-PARTY NOTIFICATION OF
15 VULNERABILITIES.—Subject to the guidance issued
16 by the Director pursuant to paragraph (4), any con-
17 tractor or awardee of an agency shall provide written
18 notification to the agency and the Cybersecurity and
19 Infrastructure Security Agency if the contractor or
20 awardee has a reasonable basis to conclude that a
21 component of any Federal information system oper-
22 ated, managed, or maintained on behalf of an agen-
23 cy by the contractor or awardee on behalf of the
24 agency contains a security vulnerability, including a
25 supply chain compromise or an identified software or

1 hardware vulnerability, that has been reported to the
2 contractor or awardee by a third party, including
3 through a vulnerability disclosure program.

4 “(3) PROCEDURES.—

5 “(A) SHARING WITH CISA.—As soon as
6 practicable following a notification of an inci-
7 dent or vulnerability to an agency by a con-
8 tractor or awardee under paragraph (1), the
9 head of the agency shall provide, pursuant to
10 section 3594, information about the incident or
11 vulnerability to the Director of the Cybersecu-
12 rity and Infrastructure Security Agency.

13 “(B) TIMING OF NOTIFICATIONS.—Unless
14 a different time for notification is specified in
15 a contract, grant, cooperative agreement, or
16 other transaction agreement, a contractor or
17 awardee shall—

18 “(i) make a notification required
19 under paragraph (1) not later than 1 day
20 after the date on which the contractor or
21 awardee has reasonable basis to suspect or
22 conclude that the criteria under paragraph
23 (1) have been met; and

24 “(ii) make a notification required
25 under paragraph (2) within a reasonable

1 time, but not later than 90 days after the
2 date on which the contractor or awardee
3 has reasonable basis to suspect or conclude
4 that the criteria under paragraph (2) have
5 been met.

6 “(C) PROCEDURES.—Following a notifica-
7 tion of a breach or incident to an agency by a
8 contractor or awardee under paragraph (1), the
9 head of the agency, in consultation with the
10 contractor or awardee, shall carry out the appli-
11 cable requirements under sections 3592, 3593,
12 and 3594 with respect to the breach or inci-
13 dent.

14 “(D) RULE OF CONSTRUCTION.—Nothing
15 in subparagraph (B) shall be construed to allow
16 the negation of the requirements to notify
17 vulnerabilities under paragraph (1) or (2)
18 through a contract, grant, cooperative agree-
19 ment, or other transaction agreement.

20 “(4) GUIDANCE.—The Director shall issue
21 guidance as soon as practicable to agencies relating
22 to the scope of vulnerabilities to be included in re-
23 quired notifications under paragraph (2), such as
24 the minimum severity or minimum risk level of a
25 vulnerability included in required notifications,

1 whether vulnerabilities that are already publicly dis-
2 closed must be reported, or likely cybersecurity im-
3 pact to Federal information systems.

4 “(b) REGULATIONS; MODIFICATIONS.—

5 “(1) IN GENERAL.—Not later than 2 years
6 after the date of enactment of the Federal Informa-
7 tion Security Modernization Act of 2024—

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

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

19 “(2) IMPLEMENTATION.—Not later than 1 year
20 after the date on which the Federal Acquisition Reg-
21 ulatory Council and the Office of Federal Financial
22 Management promulgates regulations under para-
23 graph (1), the head of each agency shall implement
24 policies and procedures, as appropriate, necessary to
25 implement those regulations.

1 “(3) CONGRESSIONAL NOTIFICATION.—

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

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

17 “(c) ALLOWABLE USE.—Information provided to an
18 agency pursuant to this section may be disclosed to, re-
19 tained by, and used by any agency, component, officer,
20 employee, or agent of the Federal Government solely for
21 any of the following:

22 “(1) A cybersecurity purpose (as defined in sec-
23 tion 2200 of the Homeland Security Act of 2002 (6
24 U.S.C. 650)).

25 “(2) Identifying—

1 “(A) a cyber threat (as defined in such
2 section 2200), including the source of the cyber
3 threat; or

4 “(B) a security vulnerability (as defined in
5 such section 2200).

6 “(3) Preventing, investigating, disrupting, or
7 prosecuting an offense arising out of an incident no-
8 tified to an agency pursuant to this section or any
9 of the offenses listed in section 105(d)(5)(A)(v) of
10 the Cybersecurity Information Sharing Act of 2015
11 (6 U.S.C. 1504(d)(5)(A)(v)).

12 “(d) HARMONIZATION OF OTHER PRIVATE-SECTOR
13 CYBERSECURITY REPORTING OBLIGATIONS.—Any non-
14 Federal entity required to report an incident under section
15 2242 of the Homeland Security Act of 2002 (6 U.S.C.
16 681b) may submit as part of the written notification re-
17 quirements in this section all information required by such
18 section 2242 to the agency of which the entity is a con-
19 tractor or recipient of Federal financial assistance, or with
20 which the entity holds an other transaction agreement or
21 cooperative agreement, within the deadline specified in
22 subsection (a)(3)(B)(1). If such submission is completed,
23 the non-Federal entity shall not be required to subse-
24 quently report the same incident under the requirements
25 of such section 2242. Any incident information shared

1 under this subsection shall be shared with the Director
2 of the Cybersecurity and Infrastructure Security Agency
3 pursuant to subsection (a)(3)(A).

4 “(e) NATIONAL SECURITY SYSTEMS EXEMPTION.—
5 Notwithstanding any other provision of this section, a con-
6 tractor or awardee of an agency that would be required
7 to report an incident or vulnerability pursuant to this sec-
8 tion that occurs exclusively on a national security system
9 shall—

10 “(1) report the incident or vulnerability to the
11 head of the agency and the Secretary of Defense;
12 and

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

15 **“§ 3596. Training**

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

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

22 “(2) an employee of a contractor or awardee of
23 an agency.

24 “(b) BEST PRACTICES AND CONSISTENCY.—The Di-
25 rector of the Cybersecurity and Infrastructure Security

1 Agency, in consultation with the Director, the National
2 Cyber Director, and the Director of the National Institute
3 of Standards and Technology, shall consolidate best prac-
4 tices to support consistency across agencies in cybersecu-
5 rity incident response training, including—

6 “(1) information to be collected and shared
7 with the Cybersecurity and Infrastructure Security
8 Agency pursuant to section 3594(a) and processes
9 for sharing such information; and

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

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

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

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

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

1 **“§ 3597. Analysis and report on Federal incidents**

2 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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

11 “(i) attacker tactics, techniques, and
12 procedures; and

13 “(ii) system vulnerabilities, including
14 zero days, unpatched systems, and infor-
15 mation system misconfigurations;

16 “(B) the scope and scale of incidents at
17 agencies;

18 “(C) common root causes of incidents
19 across multiple agencies;

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

23 “(E) lessons learned and recommendations
24 in responding to, recovering from, remediating,
25 and mitigating future incidents; and

1 “(F) trends across multiple agencies to ad-
2 dress intrusion detection and incident response
3 capabilities using the metrics established under
4 section 224(c) of the Cybersecurity Act of 2015
5 (6 U.S.C. 1522(c)).

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

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

11 “(A) IN GENERAL.—The Director of the
12 Cybersecurity and Infrastructure Security
13 Agency shall share on an ongoing basis the
14 analyses and underlying data required under
15 this subsection with agencies, the Director, and
16 the National Cyber Director to—

17 “(i) improve the understanding of cy-
18 bersecurity risk of agencies; and

19 “(ii) support the cybersecurity im-
20 provement efforts of agencies.

21 “(B) FORMAT.—In carrying out subpara-
22 graph (A), the Director of the Cybersecurity
23 and Infrastructure Security Agency shall share
24 the analyses—

1 “(i) in human-readable written prod-
2 ucts; and

3 “(ii) to the greatest extent practicable,
4 in machine-readable formats in order to
5 enable automated intake and use by agen-
6 cies.

7 “(C) EXEMPTION.—This subsection shall
8 not apply to incidents that occur exclusively on
9 national security systems.

10 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—
11 Not later than 2 years after the date of enactment of this
12 section, and not less frequently than annually thereafter,
13 the Director of the Cybersecurity and Infrastructure Secu-
14 rity Agency, in consultation with the Director, the Na-
15 tional Cyber Director and the heads of other agencies, as
16 appropriate, shall submit to the appropriate reporting en-
17 tities a report that includes—

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

21 “(2) the quantitative and qualitative analyses of
22 incidents developed under subsection (a)(1) on an
23 agency-by-agency basis and comprehensively across
24 the Federal Government, including—

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

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

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

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

7 “(B) the total number of incidents of the
8 agency; and

9 “(C) an analysis of the agency’s perform-
10 ance against the metrics established under sec-
11 tion 224(c) of the Cybersecurity Act of 2015 (6
12 U.S.C. 1522(c)).

13 “(c) PUBLICATION.—

14 “(1) IN GENERAL.—The Director of the Cyber-
15 security and Infrastructure Security Agency shall
16 make a version of each report submitted under sub-
17 section (b) publicly available on the website of the
18 Cybersecurity and Infrastructure Security Agency
19 during the year during which the report is sub-
20 mitted.

21 “(2) EXEMPTION.—The publication require-
22 ment under paragraph (1) shall not apply to a por-
23 tion of a report that contains content that should be
24 protected in the interest of national security, as de-
25 termined by the Director, the Director of the Cyber-

1 security and Infrastructure Security Agency, or the
2 National Cyber Director.

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

7 “(4) REQUIREMENT FOR COMPILING INFORMA-
8 TION.—

9 “(A) COMPILATION.—Subject to subpara-
10 graph (B), in making a report publicly available
11 under paragraph (1), the Director of the Cyber-
12 security and Infrastructure Security Agency
13 shall sufficiently compile information so that no
14 specific incident of an agency can be identified.

15 “(B) EXCEPTION.—The Director of the
16 Cybersecurity and Infrastructure Security
17 Agency may include information that enables a
18 specific incident of an agency to be identified in
19 a publicly available report—

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

22 “(ii) in consultation with the impacted
23 agency, which may, as appropriate, consult
24 with any non-Federal entity impacted by

1 or supporting the remediation of such inci-
2 dent; and

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

5 “(d) INFORMATION PROVIDED BY AGENCIES.—

6 “(1) IN GENERAL.—The analysis required
7 under subsection (a) and each report submitted
8 under subsection (b) shall use information provided
9 by agencies under section 3594(a).

10 “(2) NONCOMPLIANCE REPORTS.—During any
11 year during which the head of an agency does not
12 provide data for an incident to the Cybersecurity
13 and Infrastructure Security Agency in accordance
14 with section 3594(a), the head of the agency, in co-
15 ordination with the Director of the Cybersecurity
16 and Infrastructure Security Agency and the Direc-
17 tor, shall submit to the appropriate reporting enti-
18 ties a report that includes the information described
19 in subsection (b) with respect to the agency.

20 “(e) NATIONAL SECURITY SYSTEM REPORTS.—

21 “(1) IN GENERAL.—Notwithstanding any other
22 provision of this section, the Secretary of Defense, in
23 consultation with the Director, the National Cyber
24 Director, the Director of National Intelligence, and
25 the Director of the Cybersecurity and Infrastructure

1 Security Agency shall annually submit a report that
2 includes the information described in subsection (b)
3 with respect to national security systems, to the ex-
4 tent that the submission is consistent with standards
5 and guidelines for national security systems issued
6 in accordance with law and as directed by the Presi-
7 dent, 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 Committee on Homeland Security
13 and Governmental Affairs of the Senate;

14 “(D) the Select Committee on Intelligence
15 of the Senate;

16 “(E) the Committee on Armed Services of
17 the Senate;

18 “(F) the Committee on Appropriations of
19 the Senate;

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

22 “(H) the Committee on Homeland Security
23 of the House of Representatives;

24 “(I) the Permanent Select Committee on
25 Intelligence of the House of Representatives;

1 “(J) the Committee on Armed Services of
2 the House of Representatives; and

3 “(K) the Committee on Appropriations of
4 the House of Representatives.

5 “(2) CLASSIFIED FORM.—A report required
6 under paragraph (1) may be submitted in a classi-
7 fied form.

8 **“§ 3598. Major incident definition**

9 “(a) IN GENERAL.—Not later than 1 year after the
10 later of the date of enactment of the Federal Information
11 Security Modernization Act of 2024 and the most recent
12 publication by the Director of guidance to agencies regard-
13 ing major incidents as of the date of enactment of the
14 Federal Information Security Modernization Act of 2024,
15 the Director shall develop, in coordination with the Na-
16 tional Cyber Director, and promulgate guidance on the
17 definition of the term ‘major incident’ for the purposes
18 of subchapter II and this subchapter.

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

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

1 “(A) any incident the head of the agency
2 determines is likely to result in demonstrable
3 harm to—

4 “(i) the national security interests,
5 foreign relations, homeland security, or
6 economic security of the United States; or

7 “(ii) the civil liberties, public con-
8 fidence, privacy, or public health and safe-
9 ty of the people of the United States;

10 “(B) any incident the head of the agency
11 determines likely to result in an inability or
12 substantial disruption for the agency, a compo-
13 nent of the agency, or the Federal Government,
14 to provide 1 or more critical services;

15 “(C) any incident the head of the agency
16 determines substantially disrupts or substan-
17 tially degrades the operations of a high value
18 asset owned or operated by the agency;

19 “(D) any incident involving the exposure to
20 a foreign entity of sensitive agency information,
21 such as the communications of the head of the
22 agency, the head of a component of the agency,
23 or the direct reports of the head of the agency
24 or the head of a component of the agency; and

1 “(E) any other type of incident determined
2 appropriate by the Director;

3 “(2) stipulate that the National Cyber Director,
4 in consultation with the Director and the Director of
5 the Cybersecurity and Infrastructure Security Agen-
6 cy, may declare a major incident at any agency, and
7 such a declaration shall be considered if it is deter-
8 mined that an incident—

9 “(A) occurs at not less than 2 agencies;
10 and

11 “(B) is enabled by—

12 “(i) a common technical root cause,
13 such as a supply chain compromise, or a
14 common software or hardware vulner-
15 ability; or

16 “(ii) the related activities of a com-
17 mon threat actor;

18 “(3) stipulate that, in determining whether an
19 incident constitutes a major incident under the
20 standards described in paragraph (1), the head of
21 the agency shall consult with the National Cyber Di-
22 rector; and

23 “(4) stipulate that the mere report of a vulner-
24 ability discovered or disclosed without a loss of con-

1 confidentiality, integrity, or availability shall not on its
2 own constitute a major incident.

3 “(c) EVALUATION AND UPDATES.—Not later than 60
4 days after the date on which the Director first promul-
5 gates the guidance required under subsection (a), and not
6 less frequently than once during the first 90 days of each
7 evenly numbered Congress thereafter, the Director shall
8 provide to the Committee on Homeland Security and Gov-
9 ernmental Affairs of the Senate and the Committees on
10 Oversight and Accountability and Homeland Security of
11 the House of Representatives a briefing that includes—

12 “(1) an evaluation of any necessary updates to
13 the guidance;

14 “(2) an evaluation of any necessary updates to
15 the definition of the term ‘major incident’ included
16 in the guidance; and

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

19 (2) CLERICAL AMENDMENT.—The table of sec-
20 tions for chapter 35 of title 44, United States Code,
21 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.”.

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

2 (a) MODERNIZING GOVERNMENT TECHNOLOGY.—
3 Subtitle G of title X of division A of the National Defense
4 Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301
5 note) is amended in section 1078—

6 (1) by striking subsection (a) and inserting the
7 following:

8 “(a) DEFINITIONS.—In this section:

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

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

15 (2) in subsection (b), by adding at the end the
16 following:

17 “(8) PROPOSAL EVALUATION.—The Director
18 shall—

19 “(A) give consideration for the use of
20 amounts in the Fund to improve the security of
21 high value assets; and

22 “(B) require that any proposal for the use
23 of amounts in the Fund includes, as appro-
24 priate, and which may be incorporated into oth-
25 erwise required project proposal documenta-
26 tion—

1 “(i) cybersecurity risk management
2 considerations; and

3 “(ii) a supply chain risk assessment in
4 accordance with section 1326 of title 41.”;
5 and

6 (3) in subsection (c)—

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

10 (B) in paragraph (5)—

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

13 (ii) in subparagraph (B), by striking
14 the period at the end and inserting “and”;
15 and

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

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

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

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

3 (1) in section 11302—

4 (A) in subsection (b), by striking “use, se-
5 curity, and disposal of” and inserting “use, and
6 disposal of, and, in consultation with the Direc-
7 tor of the Cybersecurity and Infrastructure Se-
8 curity Agency and the National Cyber Director,
9 promote and improve the security of,”; and

10 (B) in subsection (h), by inserting “, in-
11 cluding cybersecurity performances,” after “the
12 performances”; and

13 (2) in section 11303(b)(2)(B)—

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

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

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

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

22 (c) SUBCHAPTER II.—Subchapter II of chapter 113
23 of subtitle III of title 40, United States Code, is amend-
24 ed—

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

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

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

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

11 **SEC. 5. ACTIONS TO ENHANCE FEDERAL INCIDENT TRANS-**
12 **PARENCY.**

13 (a) RESPONSIBILITIES OF THE CYBERSECURITY AND
14 INFRASTRUCTURE SECURITY AGENCY.—

15 (1) IN GENERAL.—Not later than 180 days
16 after the date of enactment of this Act, the Director
17 of the Cybersecurity and Infrastructure Security
18 Agency shall—

19 (A) develop a plan for the development,
20 using systems in place on the date of enactment
21 of this Act, of the analysis required under sec-
22 tion 3597(a) of title 44, United States Code, as
23 added by this Act, and the report required
24 under subsection (b) of that section that in-
25 cludes—

1 (i) a description of any challenges the
2 Director of the Cybersecurity and Infra-
3 structure Security Agency anticipates en-
4 counterering; and

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

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

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

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

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

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

23 (1) UPDATING FISMA 2014.—Section 2 of the
24 Federal Information Security Modernization Act of

1 2014 (Public Law 113–283; 128 Stat. 3073) is
2 amended—

3 (A) by striking subsections (b) and (d);
4 and

5 (B) by redesignating subsections (c), (e),
6 and (f) as subsections (b), (c), and (d), respec-
7 tively.

8 (2) INCIDENT DATA SHARING.—

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

17 (B) REQUIREMENTS.—The guidance devel-
18 oped under subparagraph (A) shall—

19 (i) enable the efficient development
20 of—

21 (I) lessons learned and rec-
22 ommendations in responding to, recov-
23 ering from, remediating, and miti-
24 gating future incidents; and

1 (II) the report on Federal inci-
2 dents required under section 3597(b)
3 of title 44, United States Code, as
4 added by this Act; and

5 (ii) include requirements for the time-
6 liness of data production.

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

14 (3) CONTRACTOR AND AWARDEE GUIDANCE.—

15 (A) IN GENERAL.—Not later than 1 year
16 after the date of enactment of this Act, the Di-
17 rector shall issue guidance to agencies on how
18 to deconflict, to the greatest extent practicable,
19 existing regulations, policies, and procedures re-
20 lating to the responsibilities of contractors and
21 awardees established under section 3595 of title
22 44, United States Code, as added by this Act.

23 (B) EXISTING PROCESSES.—To the great-
24 est extent practicable, the guidance issued
25 under subparagraph (A) shall allow contractors

1 and awardees to use existing processes for noti-
2 fying agencies of incidents involving information
3 of the Federal Government.

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

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

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

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

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

18 **SEC. 6. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SEC-**

19 **TOR ENTITIES IMPACTED BY INCIDENTS.**

20 (a) DEFINITIONS.—In this section:

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

1 (2) SENSITIVE INFORMATION.—The term “sen-
2 sitive information” has the meaning given the term
3 by the Director in guidance issued under subsection
4 (b).

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

16 (1) the confidentiality or integrity of sensitive
17 information submitted by the reporting entity to the
18 agency pursuant to a statutory or regulatory re-
19 quirement; or

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

1 **SEC. 7. FEDERAL PENETRATION TESTING POLICY.**

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

5 **“§ 3559A. Federal penetration testing**

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

9 “(1) requires agencies to perform penetration
10 testing on information systems, as appropriate, in-
11 cluding on high value assets;

12 “(2) provides policies governing the develop-
13 ment of—

14 “(A) rules of engagement for using pene-
15 tration testing; and

16 “(B) procedures to use the results of pene-
17 tration testing to improve the cybersecurity and
18 risk management of the agency;

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

21 “(4) in no manner restricts the authority of the
22 Secretary of Homeland Security or the Director of
23 the Cybersecurity and Infrastructure Agency to con-
24 duct threat hunting pursuant to section 3553, or
25 penetration testing under this chapter.

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

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

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

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

11 (b) EXISTING GUIDANCE.—

12 (1) IN GENERAL.—Compliance with guidance
13 issued by the Director relating to penetration testing
14 before the date of enactment of this Act shall be
15 deemed to be compliant with section 3559A of title
16 44, United States Code, as added by this Act.

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

23 (3) GUIDANCE UPDATES.—Notwithstanding
24 paragraphs (1) and (2), not later than 2 years after
25 the date of enactment of this Act, the Director shall

1 review and, as appropriate, update existing guidance
2 requiring penetration testing by agencies.

3 (c) 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 3559 the fol-
6 lowing:

“3559A. Federal penetration testing.”.

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

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

14 “(A) without consent or authorization from
15 agencies; and

16 “(B) with prior consultation with the head
17 of the agency at least 72 hours in advance of
18 such testing;”.

19 **SEC. 8. VULNERABILITY DISCLOSURE POLICIES.**

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

23 **“§ 3559B. Federal vulnerability disclosure policies**

24 “(a) PURPOSE; SENSE OF CONGRESS.—

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

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

11 “(b) DEFINITIONS.—In this section:

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

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

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

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

5 “(5) VULNERABILITY DISCLOSURE REPORT.—
6 The term ‘vulnerability disclosure report’ means a
7 disclosure of a security vulnerability made to an
8 agency by a submitter.

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

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

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

19 “(A) represents a good faith effort to iden-
20 tify and report security vulnerabilities in infor-
21 mation systems; or

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

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

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

9 “(5) requirements for providing information to
10 the submitter of a vulnerability disclosure report on
11 the resolution of the vulnerability disclosure report;

12 “(6) a stipulation that the mere identification
13 by a submitter of a security vulnerability, without a
14 significant compromise of confidentiality, integrity,
15 or availability, does not constitute a major incident;
16 and

17 “(7) the applicability of the guidance to inter-
18 net of things devices owned or controlled by an
19 agency.

20 “(d) CONSULTATION.—In developing the guidance re-
21 quired under subsection (c)(3), the Director shall consult
22 with the Director of the Cybersecurity and Infrastructure
23 Security Agency.

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

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

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

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

15 “(4) as appropriate, implement the require-
16 ments of this section, in accordance with the author-
17 ity under section 3553(b)(8), as a shared service
18 available to agencies.

19 “(f) RESPONSIBILITIES OF AGENCIES.—

20 “(1) PUBLIC INFORMATION.—The head of each
21 agency shall make publicly available, with respect to
22 each internet domain under the control of the agen-
23 cy that is not a national security system and to the
24 extent consistent with the security of information
25 systems but with the presumption of disclosure—

1 “(A) an appropriate security contact; and

2 “(B) the component of the agency that is
3 responsible for the internet accessible services
4 offered at the domain.

5 “(2) VULNERABILITY DISCLOSURE POLICY.—

6 The head of each agency shall develop and make
7 publicly available a vulnerability disclosure policy for
8 the agency, which shall—

9 “(A) describe—

10 “(i) the scope of the systems of the
11 agency included in the vulnerability disclo-
12 sure policy, including for internet of things
13 devices owned or controlled by the agency;

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

16 “(iii) the type of information system
17 testing that is not authorized by the agen-
18 cy;

19 “(iv) the disclosure policy for a con-
20 tractor; and

21 “(v) the disclosure policy of the agen-
22 cy for sensitive information;

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

1 “(i) how the submitter should submit
2 the vulnerability disclosure report; and

3 “(ii) if the report is not anonymous,
4 when the reporter should anticipate an ac-
5 knowledgment of receipt of the report by
6 the agency;

7 “(C) include any other relevant informa-
8 tion; and

9 “(D) be mature in scope and cover every
10 internet accessible information system used or
11 operated by that agency or on behalf of that
12 agency.

13 “(3) IDENTIFIED SECURITY
14 VULNERABILITIES.—The head of each agency
15 shall—

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

18 “(B) commensurate with the risk posed by
19 the security vulnerability, address such security
20 vulnerability using the security vulnerability
21 management process of the agency; and

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

25 “(g) EXEMPTIONS.—

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

5 “(2) LIMITATION.—The Director and the head
6 of each agency may not publish under subsection
7 (f)(1) or include in a vulnerability disclosure policy
8 under subsection (f)(2) host names, services, infor-
9 mation systems, or other information that the Direc-
10 tor or the head of an agency, in coordination with
11 the Director and other appropriate heads of agen-
12 cies, determines would—

13 “(A) disrupt a law enforcement investiga-
14 tion;

15 “(B) endanger national security or intel-
16 ligence activities; or

17 “(C) impede national defense activities or
18 military operations.

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

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

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

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

5 “(i) REVISION OF FEDERAL ACQUISITION REGULA-
6 TION.—The Federal Acquisition Regulation shall be re-
7 vised as necessary to implement the provisions under this
8 section.”.

9 (b) EXISTING GUIDANCE AND POLICIES.—

10 (1) IN GENERAL.—Compliance with guidance
11 issued by the Director relating to vulnerability dis-
12 closure policies before the date of enactment of this
13 Act shall be deemed to be compliance with section
14 3559B of title 44, United States Code, as added by
15 this title.

16 (2) IMMEDIATE NEW GUIDANCE NOT RE-
17 QUIRED.—Nothing in section 3559B of title 44,
18 United States Code, as added by this title, shall be
19 construed to require the Director to issue new guid-
20 ance to agencies relating to vulnerability disclosure
21 policies before the date described in paragraph (4).

22 (3) IMMEDIATE NEW POLICIES NOT RE-
23 QUIRED.—Nothing in section 3559B of title 44,
24 United States Code, as added by this title, shall be
25 construed to require the head of any agency to issue

1 new policies relating to vulnerability disclosure poli-
2 cies before the issuance of any updated guidance
3 under paragraph (4).

4 (4) GUIDANCE UPDATE.—Notwithstanding
5 paragraphs (1), (2) and (3), not later than 4 years
6 after the date of enactment of this Act, the Director
7 shall review and, as appropriate, update existing
8 guidance relating to vulnerability disclosure policies.

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

“3559B. Federal vulnerability disclosure policies.”.

13 (d) CONFORMING UPDATE AND REPEAL.—

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

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

23 (A) by striking section 6 (15 U.S.C. 278g–
24 3d); and

1 (B) by striking section 7 (15 U.S.C. 278g–
2 3e).

3 **SEC. 9. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

4 (a) BRIEFINGS.—Not later than 1 year after the date
5 of enactment of this Act, the Director shall provide to the
6 Committee on Homeland Security and Governmental Af-
7 fairs of the Senate and the Committees on Oversight and
8 Accountability and Homeland Security of the House of
9 Representatives a briefing on progress in increasing the
10 internal defenses of agency systems, including—

11 (1) shifting away from trusted networks to im-
12 plement security controls based on a presumption of
13 compromise, including through the transition to zero
14 trust architecture;

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

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

20 (4) identifying incidents quickly;

21 (5) isolating and removing unauthorized entities
22 from agency systems as quickly as practicable, ac-
23 counting for intelligence or law enforcement pur-
24 poses; and

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

3 (b) **PROGRESS REPORT.**—As a part of each report
4 required to be submitted under section 3553(c) of title 44,
5 United States Code, during the period beginning on the
6 date that is 4 years after the date of enactment of this
7 Act and ending on the date that is 10 years after the date
8 of enactment of this Act, the Director shall include an up-
9 date on agency implementation of zero trust architecture,
10 which shall include—

11 (1) a description of steps agencies have com-
12 pleted, including progress toward achieving any re-
13 quirements issued by the Director, including the
14 adoption of any models or reference architecture;

15 (2) an identification of activities that have not
16 yet been completed and that would have the most
17 immediate security impact; and

18 (3) a schedule to implement any planned activi-
19 ties.

20 (c) **CLASSIFIED ANNEX.**—Each update required
21 under subsection (b) may include 1 or more annexes that
22 contain classified or other sensitive information, as appro-
23 priate.

24 (d) **NATIONAL SECURITY SYSTEMS.**—

1 (1) BRIEFING.—Not later than 1 year after the
2 date of enactment of this Act, the Secretary of De-
3 fense shall provide to the Committee on Homeland
4 Security and Governmental Affairs of the Senate,
5 the Committee on Oversight and Accountability of
6 the House of Representatives, the Committee on
7 Armed Services of the Senate, the Committee on
8 Armed Services of the House of Representatives, the
9 Select Committee on Intelligence of the Senate, and
10 the Permanent Select Committee on Intelligence of
11 the House of Representatives a briefing on the im-
12 plementation of zero trust architecture with respect
13 to national security systems.

14 (2) PROGRESS REPORT.—Not later than the
15 date on which each update is required to be sub-
16 mitted under subsection (b), the Secretary of De-
17 fense shall submit to the congressional committees
18 described in paragraph (1) a progress report on the
19 implementation of zero trust architecture with re-
20 spect to national security systems.

21 **SEC. 10. AUTOMATION AND ARTIFICIAL INTELLIGENCE.**

22 (a) DEFINITION.—In this section, the term “informa-
23 tion system” has the meaning given the term in section
24 3502 of title 44, United States Code.

25 (b) USE OF ARTIFICIAL INTELLIGENCE.—

1 (1) IN GENERAL.—As appropriate, the Director
2 shall issue guidance on the use of artificial intel-
3 lligence by agencies to improve the cybersecurity of
4 information systems.

5 (2) CONSIDERATIONS.—The Director and head
6 of each agency shall consider the use and capabilities
7 of artificial intelligence systems in furtherance of the
8 cybersecurity of information systems.

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

16 (c) COMPTROLLER GENERAL REPORTS.—

17 (1) IN GENERAL.—Not later than 2 years after
18 the date of enactment of this Act, the Comptroller
19 General of the United States shall submit to the ap-
20 propriate congressional committees a report on the
21 risks to the privacy of individuals and the cybersecu-
22 rity of information systems associated with the use
23 by Federal agencies of artificial intelligence systems
24 or capabilities.

1 (2) STUDY.—Not later than 2 years after the
2 date of enactment of this Act, the Comptroller Gen-
3 eral of the United States shall perform a study, and
4 submit to the Committees on Homeland Security
5 and Governmental Affairs and Commerce, Science,
6 and Transportation of the Senate and the Commit-
7 tees on Oversight and Accountability, Homeland Se-
8 curity, and Science, Space, and Technology of the
9 House of Representatives a report, on the use of au-
10 tomation, artificial intelligence, including generative
11 artificial intelligence, and machine-readable data
12 across the Federal Government for cybersecurity
13 purposes, including—

14 (A) the automated updating of cybersecu-
15 rity tools, sensors, or processes employed by
16 agencies under paragraphs (1), (5)(C), and
17 (8)(B) of section 3554(b) of title 44, United
18 States Code, as amended by this Act; and

19 (B) to combat social engineering attacks.

20 **SEC. 11. FEDERAL CYBERSECURITY REQUIREMENTS.**

21 (a) CODIFYING FEDERAL CYBERSECURITY REQUIRE-
22 MENTS IN TITLE 44.—

23 (1) AMENDMENT TO FEDERAL CYBERSECURITY
24 ENHANCEMENT ACT OF 2015.—Section 225 of the
25 Federal Cybersecurity Enhancement Act of 2015 (6

1 U.S.C. 1523) is amended by striking subsections (b)
2 and (c).

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

6 “(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT
7 AGENCIES.—

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

13 “(A) identify sensitive and mission critical
14 data stored by the agency consistent with the
15 inventory required under section 3505(c);

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

20 “(C) encrypt or otherwise render indeci-
21 pherable to unauthorized users the data de-
22 scribed in subparagraph (A) that is stored on
23 or transiting agency information systems;

24 “(D) implement identity and access man-
25 agement systems to ensure the security of Fed-

1 eral information systems and protect agency
2 records and data from fraud resulting from the
3 misrepresentation of identity or identity theft,
4 including—

5 “(i) a single sign-on trusted identity
6 platform for individuals accessing each
7 public website of the agency that requires,
8 at a minimum, user authentication and
9 verification services consistent with appli-
10 cable law and guidance issued by the Di-
11 rector of the Office of Management and
12 Budget who shall consider any applicable
13 standard or guideline developed by the Na-
14 tional Institute of Standards and Tech-
15 nology, which may be one developed by the
16 Administrator of General Services in con-
17 sultation with the Director of the Office of
18 Management and Budget; and

19 “(ii) multi-factor authentication, con-
20 sistent with guidance issued by the Direc-
21 tor of the Office of Management and
22 Budget who shall consider any applicable
23 standard or guideline developed by the Na-
24 tional Institute of Standards and Tech-
25 nology, for—

1 “(I) remote access to an informa-
2 tion system; and

3 “(II) each user account with ele-
4 vated privileges on an information
5 system.

6 “(2) PROHIBITION.—

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

10 “(B) PROHIBITION.—Consistent with poli-
11 cies, standards, guidelines, and directives on in-
12 formation security under this subchapter, and
13 except as provided under paragraph (3), the
14 head of an agency may not procure, obtain,
15 renew a contract to procure or obtain in any
16 amount, notwithstanding section 1905 of title
17 41, or use an internet of things device if the
18 Chief Information Officer of the agency deter-
19 mines during a review required under section
20 11319(b)(1)(C) of title 40 of a contract for an
21 internet of things device that the use of the de-
22 vice prevents compliance with the standards
23 and guidelines developed under section 4 of the
24 IoT Cybersecurity Improvement Act (15 U.S.C.
25 278g–3b) with respect to the device.

1 “(3) EXCEPTIONS.—

2 “(A) IN GENERAL.—The requirements
3 under subparagraphs (A), (B), (C), and (D)(ii)
4 of paragraph (1) shall not apply to an informa-
5 tion system for which the head of the agency,
6 without delegation, has—

7 “(i) certified to the Director with par-
8 ticularity that—

9 “(I) operational requirements ar-
10 ticultated in the certification and re-
11 lated to the information system would
12 make it excessively burdensome to im-
13 plement the cybersecurity require-
14 ment;

15 “(II) the cybersecurity require-
16 ment is not necessary to secure the
17 information system or agency infor-
18 mation stored on or transiting it; and

19 “(III) the agency has taken all
20 necessary steps to secure the informa-
21 tion system and agency information
22 stored on or transiting it; and

23 “(ii) submitted the certification de-
24 scribed in clause (i) to the appropriate con-

1 gressional committees and the authorizing
2 committees of the agency.

3 “(B) IDENTITY MANAGEMENT PLATFORM
4 WAIVER.—The head of an agency shall be in
5 compliance with the requirement under para-
6 graph (1)(D)(i) with respect to implementing a
7 single-sign on trusted identity system or plat-
8 form other than one developed by the Adminis-
9 trator of General Services as described under
10 paragraph (1)(D)(i) if the head of the agency—

11 “(i) without delegation—

12 “(I) has certified to the Director
13 that the alternative system or plat-
14 form, including a procured system or
15 platform, conforms with applicable se-
16 curity and privacy requirements of
17 this subchapter and guidance issued
18 by the Director, at least 30 days be-
19 fore use of the system or platform; or

20 “(II) with regard to a system or
21 platform in use as of the date of en-
22 actment of this subsection, the head
23 of the agency provides such certifi-
24 cation to the Director within 60 days

1 after the date of enactment of this
2 subsection;

3 “(ii) has received a written waiver
4 from the Director in response to the re-
5 quest submitted under clause (i); and

6 “(iii) has submitted the certification
7 described in clause (i) and the waiver de-
8 scribed clause (ii) to the appropriate con-
9 gressional committees and the authorizing
10 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).

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) PRESUMPTION OF ADEQUACY.—A
24 FedRAMP authorization issued pursuant to chapter
25 36 of title 44 shall be presumed adequate to fulfill

1 the requirements under subparagraphs (A) through
2 (C) of paragraph (1) with respect to an agency au-
3 thorization to operate cloud computing products and
4 services if such presumption of adequacy does not
5 alter or modify—

6 “(A) the responsibility of any agency to en-
7 sure compliance with this subchapter for any
8 cloud computing product or service used by the
9 agency; or

10 “(B) the authority of the head of any
11 agency to make a determination that there is a
12 demonstrable need to include additional security
13 controls beyond those included in a FedRAMP
14 authorization package for a particular cloud
15 computing product or service.

16 “(6) RULES OF CONSTRUCTION.—Nothing in
17 this subsection shall be construed—

18 “(A) to alter the authority of the Sec-
19 retary, the Director, or the Director of the Na-
20 tional Institute of Standards and Technology in
21 implementing subchapter II of this title;

22 “(B) to affect the standards or process of
23 the National Institute of Standards and Tech-
24 nology;

1 “(C) to affect the requirement under sec-
2 tion 3553(a)(4);

3 “(D) to discourage continued improve-
4 ments and advancements in the technology,
5 standards, policies, and guidelines used to pro-
6 mote Federal information security; or

7 “(E) to affect the requirements under sub-
8 chapter III.

9 “(g) EXCEPTION.—

10 “(1) NATIONAL SECURITY SYSTEM REQUIRE-
11 MENTS.—The requirements under subsection (f)(1)
12 shall not apply to—

13 “(A) a national security system; or

14 “(B) an information system described in
15 paragraph (2) or (3) of section 3553(e)(2).

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

18 “(A) necessary in the interest of national
19 security;

20 “(B) national security systems; or

21 “(C) a procured internet of things device
22 described in subsection (f)(2)(B) that the Chief
23 Information Officer of an agency determines
24 is—

25 “(i) necessary for research purposes;

1 “(ii) necessary in the interest of na-
2 tional security; or

3 “(iii) secured using alternative and ef-
4 fective methods appropriate to the function
5 of the internet of things device.”.

6 (b) REPORT ON EXEMPTIONS.—Section 3554(c)(1)
7 of title 44, United States Code, as amended by this Act,
8 is further amended—

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

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

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

14 “(D) with respect to any exemption from
15 the requirements of subsection (f)(3) that is ef-
16 fective on the date of submission of the report,
17 includes the number of information systems
18 that have received an exemption from those re-
19 quirements.”.

20 (c) GUIDANCE FOR IDENTITY MANAGEMENT SYS-
21 TEMS USED BY AGENCIES.—Not later than 1 year after
22 the date of enactment of this Act, the Director of the Of-
23 fice of Management and Budget, in consultation with the
24 Director of the National Institute of Standards and Tech-
25 nology, shall issue, and routinely update thereafter, guid-

1 ance for agencies to implement identity management sys-
2 tems and a single sign-on trusted identity platform as re-
3 quired under section 3554(f)(1)(D)(i) of title 44, United
4 States Code, as amended by this Act, which shall at a min-
5 imum, include the following:

6 (1) Requirements for agencies to routinely cer-
7 tify that such systems are in compliance with this
8 guidance.

9 (2) Requirements for agencies to routinely
10 verify and certify that information stored on or
11 transiting through a commercially available product
12 (as defined in section 103 of title 41, United States
13 Code) or commercial service (as defined in section
14 103a of title 41, United States Code) used to fulfil
15 such requirements is appropriately secured in con-
16 formity with subchapter II of chapter 35 of title 44,
17 United States Code.

18 (3) Address national security concerns and re-
19 quirements to ensure the protection of sensitive per-
20 sonal records and biometric data of United States
21 persons from malign foreign ownership, control, or
22 influence and fraud actors.

23 (4) Requirements or guidelines to comply with
24 section 3 of the 21st Century Idea Act (44 U.S.C.
25 3501 note).

1 (5) Requirements to prevent discrimination in
2 violation of title VI of the Civil Rights Act of 1964
3 (42 U.S.C. 2000d et seq.).

4 (6) A description of the information necessary
5 to be submitted under the exception described in sec-
6 tion 3554(f)(3)(B) of title 44, United States Code,
7 as amended by this Act.

8 (d) GAO EVALUATION OF TECHNICAL CAPABILITY
9 OF IDENTITY MANAGEMENT SYSTEMS AND PLAT-
10 FORMS.—Not less frequently than every 3 years for the
11 next 6 years, the Comptroller General shall submit to the
12 appropriate congressional committees a report on whether
13 the single sign-on trusted identity systems and platforms
14 used by agencies or the one developed by the General Serv-
15 ices Administration under section 3554(f)(D)(i) of title
16 44, United States Code, as amended by this Act, adhere
17 to the information security requirements of chapter 35 of
18 title 44, United States Code, guidance issued under sub-
19 section (c), and relevant identity management technical
20 standards promulgated by the National Institute of Stand-
21 ards and Technology, as appropriate, including section
22 504 of the Cybersecurity Enhancement Act of 2014 (15
23 U.S.C. 7464).

24 (e) 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 (f) 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. 12. 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 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. 13. 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”;

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 (C) in paragraph (17), by striking “E-
6 Government” and inserting “annual”; and

7 (8) in subsection (g), by striking “the Office of
8 Electronic Government” and inserting “the Office of
9 the Federal Chief Information Officer”.

10 (c) CHIEF INFORMATION OFFICERS COUNCIL.—Sec-
11 tion 3603 of title 44, United States Code, is amended—

12 (1) in subsection (b)(2), by striking “The Ad-
13 ministrator of the Office of Electronic Government”
14 and inserting “The Federal Chief Information Offi-
15 cer”;

16 (2) in subsection (c)(1), by striking “The Ad-
17 ministrator of the Office of Electronic Government”
18 and inserting “The Federal Chief Information Offi-
19 cer”; and

20 (3) in subsection (f)—

21 (A) in paragraph (3), by striking “the Ad-
22 ministrator” and inserting “the Federal Chief
23 Information Officer”; and

1 (B) in paragraph (5), by striking “the Ad-
2 ministrator” and inserting “the Federal Chief
3 Information Officer”.

4 (d) E-GOVERNMENT FUND.—Section 3604 of title
5 44, United States Code, is amended—

6 (1) in subsection (a)(2), by striking “the Ad-
7 ministrator of the Office of Electronic Government”
8 and inserting “the Federal Chief Information Offi-
9 cer”;

10 (2) in subsection (b), by striking “Adminis-
11 trator” each place it appears and inserting “Federal
12 Chief Information Officer”; and

13 (3) in subsection (c), in the matter preceding
14 paragraph (1), by striking “the Administrator” and
15 inserting “the Federal Chief Information Officer”.

16 (e) PROGRAM TO ENCOURAGE INNOVATIVE SOLU-
17 TIONS TO ENHANCE ELECTRONIC GOVERNMENT SERV-
18 ICES AND PROCESSES.—Section 3605 of title 44, United
19 States Code, is amended—

20 (1) in subsection (a), by striking “The Adminis-
21 trator” and inserting “The Federal Chief Informa-
22 tion Officer”;

23 (2) in subsection (b), by striking “, the Admin-
24 istrator,” and inserting “, the Federal Chief Infor-
25 mation Officer,”; and

1 (3) in subsection (c)—

2 (A) in paragraph (1)—

3 (i) by striking “The Administrator”
4 and inserting “The Federal Chief Informa-
5 tion Officer”; and

6 (ii) by striking “proposals submitted
7 to the Administrator” and inserting “pro-
8 posals submitted to the Federal Chief In-
9 formation Officer”;

10 (B) in paragraph (2)(B), by striking “the
11 Administrator” and inserting “the Federal
12 Chief Information Officer”; and

13 (C) in paragraph (4), by striking “the Ad-
14 ministrator” and inserting “the Federal Chief
15 Information Officer”.

16 (f) E-GOVERNMENT REPORT.—Section 3606 of title
17 44, United States Code, is amended—

18 (1) in the section heading by striking “**E-Gov-**
19 **ernment**” and inserting “**Annual**”;

20 (2) in subsection (a), by striking “E-Govern-
21 ment” and inserting “annual”; and

22 (3) in subsection (b)(1), by striking “202(f)”
23 and inserting “202(g)”.

24 (g) TREATMENT OF INCUMBENT.—The individual
25 serving as the Administrator of the Office of Electronic

1 Government under section 3602 of title 44, United States
2 Code, as of the date of enactment of this Act, may con-
3 tinue to serve as the Federal Chief Information Officer
4 commencing as of that date, without need for a further
5 or additional appointment under such section.

6 (h) TECHNICAL AND CONFORMING AMENDMENTS.—
7 The table of sections for chapter 36 of title 44, United
8 States Code, is amended—

9 (1) by striking the item relating to section 3602
10 and inserting the following:

“3602. Office of the Federal Chief Information Officer.”;

11 and

12 (2) in the item relating to section 3606, by
13 striking “E–Government” and inserting “Annual”.

14 (i) REFERENCES.—

15 (1) ADMINISTRATOR.—Any reference to the Ad-
16 ministrator of the Office of Electronic Government
17 in any law, regulation, map, document, record, or
18 other paper of the United States shall be deemed to
19 be a reference to the Federal Chief Information Offi-
20 cer.

21 (2) OFFICE OF ELECTRONIC GOVERNMENT.—
22 Any reference to the Office of Electronic Govern-
23 ment in any law, regulation, map, document, record,
24 or other paper of the United States shall be deemed

1 to be a reference to the Office of the Federal Chief
2 Information Officer.

3 **SEC. 14. RULES OF CONSTRUCTION.**

4 (a) AGENCY ACTIONS.—Nothing in this Act, or an
5 amendment made by this Act, shall be construed to au-
6 thorize the head of an agency to take an action that is
7 not authorized by this Act, an amendment made by this
8 Act, or existing law.

9 (b) PROTECTION OF RIGHTS.—Nothing in this Act,
10 or an amendment made by this Act, shall be construed
11 to permit the violation of the rights of any individual pro-
12 tected by the Constitution of the United States, including
13 through censorship of speech protected by the Constitu-
14 tion of the United States or unauthorized surveillance.

15 (c) PROTECTION OF PRIVACY.—Nothing in this Act,
16 or any amendment made by this Act, shall be construed
17 to—

18 (1) impinge on the privacy rights of individuals;

19 or

20 (2) allow the unauthorized access, sharing, or
21 use of personal data.

