

Union Calendar No. 790

118TH CONGRESS
2^D SESSION

H. R. 4552

[Report No. 118–939, Part I]

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

IN THE HOUSE OF REPRESENTATIVES

JULY 11, 2023

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

DECEMBER 19, 2024

Additional sponsor: Mr. DAVIS of North Carolina

DECEMBER 19, 2024

Reported from the Committee on Oversight and Accountability with an amendment

[Strike out all after the enacting clause and insert the part printed in *italie*]

DECEMBER 19, 2024

Committees on Science, Space, and Technology, Homeland Security, and Armed Services discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on July 11, 2023]

A BILL

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

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

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

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

6 (b) *TABLE OF CONTENTS.*—*The table of contents for*
 7 *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 inci-
dents.

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.

8 **SEC. 2. DEFINITIONS.**

9 *In this Act, unless otherwise specified:*

10 (1) *AGENCY.*—*The term “agency” has the mean-*
 11 *ing given the term in section 3502 of title 44, United*
 12 *States Code.*

13 (2) *APPROPRIATE CONGRESSIONAL COMMIT-*
 14 *TEES.*—*The term “appropriate congressional commit-*
 15 *tees” means—*

16 (A) *the Committee on Homeland Security*
 17 *and Governmental Affairs of the Senate;*

1 (B) *the Committee on Oversight and Ac-*
2 *countability of the House of Representatives; and*

3 (C) *the Committee on Homeland Security of*
4 *the House of Representatives.*

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

8 (4) *CONTRACTOR.*—*The term “contractor” has*
9 *the meaning given the term in section 3591 of title*
10 *44, United States Code, as added by this Act.*

11 (5) *DIRECTOR.*—*The term “Director” means the*
12 *Director of the Office of Management and Budget.*

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

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

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

24 (9) *PENETRATION TEST.*—*The term “penetration*
25 *test” has the meaning given the term in section*

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

3 (10) *THREAT HUNTING*.—The term “threat hunt-
4 ing” means proactively and iteratively searching sys-
5 tems for threats and vulnerabilities, including threats
6 or vulnerabilities that may evade detection by auto-
7 mated threat detection systems.

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

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

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

16 (1) in section 3504—

17 (A) in subsection (a)(1)(B)—

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

20 “(v) privacy, confidentiality, disclosure,
21 and sharing of information;”;

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

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

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

4 (B) in subsection (g)—

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

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

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

13 “(2) in consultation with the National Cyber Di-
14 rector, oversee the implementation of policies, prin-
15 ciples, standards, and guidelines on security, of infor-
16 mation collected or maintained by or for agencies;
17 and”;

18 (2) in section 3505—

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

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

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

3 (i) in subparagraph (B)—

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

9 (II) by striking “and” at the end;

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

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

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

18 (3) in section 3506—

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

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

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

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

6 “(j)(1) Notwithstanding paragraphs (2) and (3) of
7 subsection (a), the head of each agency shall, in accordance
8 with section 522(a) of division H of the Consolidated Ap-
9 propriations Act, 2005 (42 U.S.C. 2000ee-2), designate a
10 Chief Privacy Officer with the necessary skills, knowledge,
11 and expertise, who shall have the authority and responsi-
12 bility to—

13 “(A) lead the privacy program of the agency;
14 and

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

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

19 “(A) serve in a central leadership position with-
20 in the agency;

21 “(B) have visibility into relevant agency oper-
22 ations; and

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

1 “(3) A privacy officer of an agency established under
2 a statute enacted before the date of enactment of the Federal
3 Information Security Modernization Act of 2024 may carry
4 out the responsibilities under this subsection for the agen-
5 cy.”; and

6 (4) in section 3513—

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

9 (B) by inserting after subsection (b) the fol-
10 lowing:

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

15 (b) SUBCHAPTER II DEFINITIONS.—

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

18 (A) by redesignating paragraphs (2), (3),
19 (4), (5), (6), and (7) as paragraphs (3), (4), (5),
20 (6), (8), and (10), respectively;

21 (B) by inserting after paragraph (1) the fol-
22 lowing:

23 “(2) The term ‘high value asset’ means informa-
24 tion or an information system that the head of an
25 agency, using policies, principles, standards, or

1 *guidelines issued by the Director under section*
2 *3553(a), determines to be so critical to the agency*
3 *that the loss or degradation of the confidentiality, in-*
4 *tegrity, or availability of such information or infor-*
5 *mation system would have a serious impact on the*
6 *ability of the agency to perform the mission of the*
7 *agency or conduct business.”;*

8 *(C) by inserting after paragraph (6), as so*
9 *redesignated, the following:*

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

13 *(D) in paragraph (8)(A), as so redesign-*
14 *ated, in the matter preceding clause (i), by*
15 *striking “used” and inserting “owned, man-*
16 *aged,”;*

17 *(E) by inserting after paragraph (8), as so*
18 *redesignated, the following:*

19 *“(9) The term ‘penetration test’—*

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

1 “(B) includes any additional meaning
2 given the term in policies, principles, standards,
3 or guidelines issued by the Director under section
4 3553(a).”; and

5 (F) by inserting after paragraph (10), as so
6 redesignated, the following:

7 “(11) The term ‘shared service’ means a central-
8 ized mission capability or consolidated business func-
9 tion that is provided to multiple organizations within
10 an agency or to multiple agencies.

11 “(12) The term ‘zero trust architecture’ has the
12 meaning given the term in Special Publication 800-
13 207 of the National Institute of Standards and Tech-
14 nology, or any successor document.”.

15 (2) CONFORMING AMENDMENTS.—

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

21 (B) TITLE 10.—

22 (i) SECTION 2222.—Section 2222(i)(8)
23 of title 10, United States Code, is amended
24 by striking “section 3552(b)(6)(A)” and in-
25 serting “section 3552(b)(8)(A)”.

1 (ii) *SECTION 2223.—Section 2223(c)(3)*
2 *of title 10, United States Code, is amended*
3 *by striking “section 3552(b)(6)” and insert-*
4 *ing “section 3552(b)”.*

5 (iii) *SECTION 3068.—Section 3068(b) of*
6 *title 10, United States Code, is amended by*
7 *striking “section 3552(b)(6)” and inserting*
8 *“section 3552(b)”.*

9 (iv) *SECTION 3252.—Section 3252(e)(5)*
10 *of title 10, United States Code, is amended*
11 *by striking “section 3552(b)(6)” and insert-*
12 *ing “section 3552(b)”.*

13 (C) *HIGH-PERFORMANCE COMPUTING ACT*
14 *OF 1991.—Section 207(a) of the High-Perform-*
15 *ance Computing Act of 1991 (15 U.S.C. 5527(a))*
16 *is amended by striking “section*
17 *3552(b)(6)(A)(i)” and inserting “section*
18 *3552(b)(8)(A)(i)”.*

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

1 (E) NATIONAL DEFENSE AUTHORIZATION
2 ACT FOR FISCAL YEAR 2013.—Section
3 933(e)(1)(B) of the National Defense Authoriza-
4 tion Act for Fiscal Year 2013 (10 U.S.C. 2224
5 note) is amended by striking “section
6 3542(b)(2)” and inserting “section 3552(b)”.

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

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

15 (ii) in section 932(b)(2) (10 U.S.C.
16 2224 note), by striking “section 3542(b)(2)”
17 and inserting “section 3552(b)”.

18 (G) E–GOVERNMENT ACT OF 2002.—Section
19 301(c)(1)(A) of the E–Government Act of 2002
20 (44 U.S.C. 3501 note) is amended by striking
21 “section 3542(b)(2)” and inserting “section
22 3552(b)”.

23 (H) NATIONAL INSTITUTE OF STANDARDS
24 AND TECHNOLOGY ACT.—Section 20 of the Na-

1 *tional Institute of Standards and Technology Act*
2 *(15 U.S.C. 278g-3) is amended—*

3 *(i) in subsection (a)(2), by striking*
4 *“section 3552(b)(6)” and inserting “section*
5 *3552(b)”;* *and*

6 *(ii) in subsection (f)—*

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

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

13 *(c) SUBCHAPTER II AMENDMENTS.—Subchapter II of*
14 *chapter 35 of title 44, United States Code, is amended—*

15 *(1) in section 3551—*

16 *(A) in paragraph (4), by striking “diagnose*
17 *and improve” and inserting “integrate, deliver,*
18 *diagnose, and improve”;*

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

21 *(C) in paragraph (6), by striking the period*
22 *at the end and inserting a semicolon; and*

23 *(D) by adding at the end the following:*

1 “(7) recognize that each agency has specific mis-
2 sion requirements and, at times, unique cybersecurity
3 requirements to meet the mission of the agency;

4 “(8) recognize that each agency does not have the
5 same resources to secure agency systems, and an agen-
6 cy should not be expected to have the capability to se-
7 cure the systems of the agency from advanced adver-
8 saries alone; and

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

12 (2) in section 3553—

13 (A) in subsection (a)—

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

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

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

21 “(7) promoting, in consultation with the Direc-
22 tor of the Cybersecurity and Infrastructure Security
23 Agency, the National Cyber Director, and the Director
24 of the National Institute of Standards and Tech-
25 nology—

1 “(A) the use of automation to improve Fed-
2 eral cybersecurity and visibility with respect to
3 the implementation of Federal cybersecurity; and

4 “(B) the use of presumption of compromise
5 and least privilege principles, such as zero trust
6 architecture, to improve resiliency and timely re-
7 sponse actions to incidents on Federal systems.”;

8 (B) in subsection (b)—

9 (i) in the matter preceding paragraph
10 (1), by inserting “and the National Cyber
11 Director” after “Director”;

12 (ii) in paragraph (2)(A), by inserting
13 “and reporting requirements under sub-
14 chapter IV of this chapter” after “section
15 3556”;

16 (iii) by redesignating paragraphs (8)
17 and (9) as paragraphs (10) and (11), re-
18 spectively; and

19 (iv) by inserting after paragraph (7)
20 the following:

21 “(8) expeditiously seeking opportunities to re-
22 duce costs, administrative burdens, and other barriers
23 to information technology security and modernization
24 for agencies, including through shared services (and
25 appropriate commercial off the shelf options for such

1 *shared services) for cybersecurity capabilities identi-*
2 *fied as appropriate by the Director, in coordination*
3 *with the Director of the Cybersecurity and Infrastruc-*
4 *ture Security Agency and other agencies as appro-*
5 *priate;”;*

6 *(C) in subsection (c)—*

7 *(i) in the matter preceding paragraph*

8 *(1)—*

9 *(I) by striking “each year” and*
10 *inserting “each year during which*
11 *agencies are required to submit reports*
12 *under section 3554(c)”;*

13 *(II) by inserting “, which shall be*
14 *unclassified but may include 1 or more*
15 *annexes that contain classified or other*
16 *sensitive information, as appropriate”*
17 *after “a report”; and*

18 *(III) by striking “preceding year”*
19 *and inserting “preceding 2 years”;*

20 *(ii) by striking paragraph (1);*

21 *(iii) by redesignating paragraphs (2),*
22 *(3), and (4) as paragraphs (1), (2), and (3),*
23 *respectively;*

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

1 (v) by inserting after paragraph (3),
2 as so redesignated, the following:

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

6 (D) in subsection (h)—

7 (i) in paragraph (2)—

8 (I) in subparagraph (A), by in-
9 serting “and the National Cyber Direc-
10 tor” after “in coordination with the
11 Director”;

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

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

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

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

1 “(i) *FEDERAL RISK ASSESSMENT.*—*On an ongoing*
2 *and continual basis, the Director of the Cybersecurity and*
3 *Infrastructure Security Agency shall assess the Federal risk*
4 *posture using any available information on the cybersecu-*
5 *rity posture of agencies, and brief the Director and National*
6 *Cyber Director on the findings of such assessment, includ-*
7 *ing—*

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 agency;*

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

15 “(4) *evaluation of penetration testing performed*
16 *under section 3559A;*

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

19 “(6) *evaluation of agency threat hunting results;*

20 “(7) *evaluation of Federal and non-Federal cyber*
21 *threat intelligence;*

22 “(8) *data on agency compliance with standards*
23 *issued under section 11331 of title 40;*

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

1 “(10) relevant reports from inspectors general of
2 agencies and the Government Accountability Office;
3 and

4 “(11) any other information the Director of the
5 Cybersecurity and Infrastructure Security Agency de-
6 termines relevant.”; and

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

8 “(m) DIRECTIVES.—

9 “(1) EMERGENCY DIRECTIVE UPDATES.—If the
10 Secretary issues an emergency directive under this
11 section, 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 an update on the status of the imple-
18 mentation of the emergency directive at agencies not
19 later than 7 days after the date on which the emer-
20 gency directive requires an agency to complete a re-
21 quirement specified by the emergency directive, and
22 every 30 days thereafter until—

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

1 “(B) the Secretary determines that an emer-
2 gency directive no longer requires active report-
3 ing from agencies or additional implementation;
4 or

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

7 “(2) *BINDING OPERATIONAL DIRECTIVE UP-*
8 *DATES.*—If the Secretary issues a binding operational
9 directive under this section, the Director of the Cyber-
10 security and Infrastructure Security Agency shall
11 submit to the Director, the National Cyber Director,
12 the Committee on Homeland Security and Govern-
13 mental Affairs of the Senate, and the Committees on
14 Oversight and Accountability and Homeland Security
15 of the House of Representatives an update on the sta-
16 tus of the implementation of the binding operational
17 directive at agencies not later than 30 days after the
18 issuance of the binding operational directive, and
19 every 90 days thereafter until—

20 “(A) the date on which every agency has
21 fully implemented the binding operational direc-
22 tive;

23 “(B) the Secretary determines that a bind-
24 ing operational directive no longer requires ac-

1 *tive reporting from agencies or additional imple-*
2 *mentation; or*

3 “(C) *the date that is 1 year after the*
4 *issuance or substantive update of the directive.*

5 “(3) *REPORT.—If the Director of the Cybersecu-*
6 *rity and Infrastructure Security Agency ceases sub-*
7 *mitting updates required under paragraphs (1) or (2)*
8 *on the date described in paragraph (1)(C) or (2)(C),*
9 *the Director of the Cybersecurity and Infrastructure*
10 *Security Agency shall submit to the Director, the Na-*
11 *tional Cyber Director, the Committee on Homeland*
12 *Security and Governmental Affairs of the Senate, and*
13 *the Committees on Oversight and Accountability and*
14 *Homeland Security of the House of Representatives a*
15 *list of every agency that, at the time of the report—*

16 “(A) *has not completed a requirement speci-*
17 *fied by an emergency directive; or*

18 “(B) *has not implemented a binding oper-*
19 *ational directive.*

20 “(n) *REVIEW OF OFFICE OF MANAGEMENT AND BUDG-*
21 *ET GUIDANCE AND POLICY.—*

22 “(1) *CONDUCT OF REVIEW.—Not less frequently*
23 *than once every 3 years, the Director of the Office of*
24 *Management and Budget shall review the efficacy of*
25 *the guidance and policy promulgated by the Director*

1 *in reducing cybersecurity risks, including a consider-*
2 *ation of reporting and compliance burden on agen-*
3 *cies.*

4 “(2) *CONGRESSIONAL NOTIFICATION.*—*The Di-*
5 *rector of the Office of Management and Budget shall*
6 *notify the Committee on Homeland Security and*
7 *Governmental Affairs of the Senate and the Com-*
8 *mittee on Oversight and Accountability of the House*
9 *of Representatives of the results of the review under*
10 *paragraph (1).*

11 “(3) *GAO REVIEW.*—*The Government Account-*
12 *ability Office shall review guidance and policy pro-*
13 *mulgated by the Director to assess its efficacy in risk*
14 *reduction and burden on agencies.*

15 “(o) *AUTOMATED STANDARD IMPLEMENTATION*
16 *VERIFICATION.*—*When the Director of the National Insti-*
17 *tute of Standards and Technology issues a proposed stand-*
18 *ard or guideline pursuant to paragraphs (2) or (3) of sec-*
19 *tion 20(a) of the National Institute of Standards and Tech-*
20 *nology Act (15 U.S.C. 278g–3(a)), the Director of the Na-*
21 *tional Institute of Standards and Technology shall consider*
22 *developing and, if appropriate and practical, develop speci-*
23 *fications to enable the automated verification of the imple-*
24 *mentation of the controls.*

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

8 (3) *in section 3554—*

9 (A) *in subsection (a)—*

10 (i) *in paragraph (1)—*

11 (I) *by redesignating subpara-*
12 *graphs (A), (B), and (C) as subpara-*
13 *graphs (B), (C), and (D), respectively;*

14 (II) *by inserting before subpara-*
15 *graph (B), as so redesignated, the fol-*
16 *lowing:*

17 “(A) *on an ongoing and continual basis, as-*
18 *sessing agency system risk, as applicable, by—*

19 “(i) *identifying and documenting the*
20 *high value assets of the agency using guid-*
21 *ance from the Director;*

22 “(ii) *evaluating the data assets inven-*
23 *toried under section 3511 for sensitivity to*
24 *compromises in confidentiality, integrity,*
25 *and availability;*

1 “(iii) identifying whether the agency is
2 participating in federally offered cybersecurity
3 shared services programs;

4 “(iv) identifying agency systems that
5 have access to or hold the data assets inven-
6 toried under section 3511;

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

12 “(vi) evaluating the vulnerability of
13 agency systems and data, including high
14 value assets, including by analyzing—

15 “(I) the results of penetration test-
16 ing performed by the Department of
17 Homeland Security under section
18 3553(b)(9);

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

21 “(III) information provided to the
22 agency through the vulnerability dis-
23 closure program of the agency under
24 section 3559B;

25 “(IV) incidents; and

1 “(V) any other vulnerability in-
2 formation relating to agency systems
3 that is known to the agency;

4 “(vii) assessing the impacts of poten-
5 tial agency incidents to agency systems,
6 data, and operations based on the evalua-
7 tions described in clauses (ii) and (v) and
8 the agency systems identified under clause
9 (iv); and

10 “(viii) assessing the consequences of po-
11 tential incidents occurring on agency sys-
12 tems that would impact systems at other
13 agencies, including due to interconnectivity
14 between different agency systems or oper-
15 ational reliance on the operations of the sys-
16 tem or data in the system;”;

17 (III) in subparagraph (B), as so
18 redesignated, in the matter preceding
19 clause (i), by striking “providing in-
20 formation” and inserting “using infor-
21 mation from the assessment required
22 under subparagraph (A), providing in-
23 formation”;

24 (IV) in subparagraph (C), as so
25 redesignated—

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

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

6 (V) in subparagraph (D), as so
7 redesignated, by inserting “and” after
8 the semicolon at the end; and

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

11 “(E) providing an update on the ongoing
12 and continual assessment required under sub-
13 paragraph (A)—

14 “(i) upon request, to the inspector gen-
15 eral of the agency or the Comptroller Gen-
16 eral of the United States; and

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

21 “(I) the Director;

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

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

3 (ii) in paragraph (2)—

4 (I) in subparagraph (A), by in-
5 serting “in accordance with the agency
6 system risk assessment required under
7 paragraph (1)(A)” after “information
8 systems”; and

9 (II) in subparagraph (D), by in-
10 serting “, through the use of penetra-
11 tion testing, the vulnerability disclo-
12 sure program established under section
13 3559B, and other means,” after “peri-
14 odically”;

15 (iii) in paragraph (3)(A)—

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

20 (II) in clause (i), by striking “this
21 section” and inserting “subsections (a)
22 through (c)”;

23 (III) in clause (ii), by striking
24 “training and” and inserting “skills,
25 training, and”;

1 (IV) by redesignating clauses (iii)
2 and (iv) as clauses (iv) and (v), respec-
3 tively;

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

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

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

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

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

24 (B) in subsection (b)—

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

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

9 (ii) in paragraph (2)—

10 (I) by striking subparagraph (B);

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

14 (III) in subparagraph (C), as so
15 redesignated—

16 (aa) by redesignating clauses
17 (iii) and (iv) as clauses (iv) and
18 (v), respectively;

19 (bb) by inserting after clause
20 (ii) the following:

21 “(iii) binding operational directives
22 and emergency directives issued by the Sec-
23 retary under section 3553;”;

24 (cc) in clause (iv), as so re-
25 designated, by striking “as deter-

1 *mined by the agency;” and insert-*
2 *ing “as determined by the agency,*
3 *considering the agency risk assess-*
4 *ment required under subsection*
5 *(a)(1)(A);”;*

6 *(iii) in paragraph (5)(A), by inserting*
7 *“, including penetration testing, as appro-*
8 *priate,” after “shall include testing”;*

9 *(iv) by redesignating paragraphs (7)*
10 *and (8) as paragraphs (8) and (9), respec-*
11 *tively;*

12 *(v) by inserting after paragraph (6)*
13 *the following:*

14 *“(7) a process for securely providing the status*
15 *of remedial cybersecurity actions and un-remediated*
16 *identified system vulnerabilities of high value assets*
17 *to the Director and the Director of the Cybersecurity*
18 *and Infrastructure Security Agency, using automa-*
19 *tion and machine-readable data as appropriate;”;*
20 *and*

21 *(vi) in paragraph (8)(C), as so redesign-*
22 *ated—*

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

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

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

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

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

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

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

15 (bb) by striking subclause
16 (III); and

17 (cc) by redesignating sub-
18 clause (IV) as subclause (III); and
19 (C) in subsection (c)—

20 (i) by redesignating paragraph (2) as
21 paragraph (4);

22 (ii) by striking paragraph (1) and in-
23 serting the following:
24

1 “(1) *BIENNIAL REPORT.*—Not later than 2 years
2 after the date of enactment of the Federal Information
3 Security Modernization Act of 2024 and not less fre-
4 quently than once every 2 years thereafter, using the
5 ongoing and continual agency system risk assessment
6 required under subsection (a)(1)(A), the head of each
7 agency shall submit to the Director, the National
8 Cyber Director, the Director of the Cybersecurity and
9 Infrastructure Security Agency, the Comptroller Gen-
10 eral of the United States, the majority and minority
11 leaders of the Senate, the Speaker and minority lead-
12 er of the House of Representatives, the Committee on
13 Homeland Security and Governmental Affairs of the
14 Senate, the Committee on Oversight and Account-
15 ability of the House of Representatives, the Committee
16 on Homeland Security of the House of Representa-
17 tives, the Committee on Commerce, Science, and
18 Transportation of the Senate, the Committee on
19 Science, Space, and Technology of the House of Rep-
20 resentatives, and the appropriate authorization and
21 appropriations committees of Congress a report
22 that—

23 “(A) summarizes the agency system risk as-
24 sessment required under subsection (a)(1)(A);

1 “(B) evaluates the adequacy and effective-
2 ness of information security policies, procedures,
3 and practices of the agency to address the risks
4 identified in the agency system risk assessment
5 required under subsection (a)(1)(A), including
6 an analysis of the agency’s cybersecurity and in-
7 cident response capabilities using the metrics es-
8 tablished under section 224(c) of the Cybersecu-
9 rity Act of 2015 (6 U.S.C. 1522(c));

10 “(C) summarizes the status of remedial ac-
11 tions identified by inspector general of the agen-
12 cy, the Comptroller General of the United States,
13 and any other source determined appropriate by
14 the head of the agency; and

15 “(D) includes the cybersecurity shared serv-
16 ices offered by the Cybersecurity and Infrastruc-
17 ture Security Agency that the agency partici-
18 pates in, if any, and explanations for any non-
19 participation in such services.

20 “(2) UNCLASSIFIED REPORTS.—Each report sub-
21 mitted under paragraph (1)—

22 “(A) shall be, to the greatest extent prac-
23 ticable, in an unclassified and otherwise uncon-
24 trolled form; and

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

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

10 (iii) in paragraph (4), as so redesign-
11 ated, by striking the period at the end and
12 inserting “, including the reporting proce-
13 dures established under section 11315(d) of
14 title 40 and subsection (a)(3)(A)(v) of this
15 section.”;

16 (4) in section 3555—

17 (A) in the section heading, by striking
18 “**Annual independent**” and inserting
19 “**Independent**”;

20 (B) in subsection (a)—

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

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

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

9 “(3) An evaluation under this section may include rec-
10 ommendations for improving the cybersecurity posture of
11 the agency.”;

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

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

17 (E) in subsection (g)(2)—

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

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

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

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

3 (F) by striking subsection (j) and inserting
4 the following:

5 “(j) GUIDANCE.—

6 “(1) IN GENERAL.—The Director, in consultation
7 with the Director of the Cybersecurity and Infrastruc-
8 ture Security Agency, the Chief Information Officers
9 Council, the Council of the Inspectors General on In-
10 tegrity and Efficiency, and other interested parties as
11 appropriate, shall ensure the development of risk-
12 based guidance for evaluating the effectiveness of an
13 information security program and practices.

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

16 “(A) the identification of the most common
17 successful threat patterns;

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

21 “(C) any other security risks unique to Fed-
22 eral systems; and

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

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

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

7 (5) *in section 3556(a)*—

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

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

14 (d) *CONFORMING AMENDMENTS.*—

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

“3555. *Independent evaluation.*”.

19 (2) *OMB REPORTS.*—*Section 226(c) of the Cy-*
20 *bersecurity Act of 2015 (6 U.S.C. 1524(c)) is amend-*
21 *ed—*

22 (A) *in paragraph (1)(B), in the matter pre-*
23 *ceding clause (i), by striking “annually there-*
24 *after” and inserting “thereafter during the years*
25 *during which a report is required to be sub-*

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

3 (B) in paragraph (2)(B), in the matter pre-
4 ceding clause (i)—

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

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

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

17 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

18 (1) IN GENERAL.—Chapter 35 of title 44, United
19 States Code, is amended by adding at the end the fol-
20 lowing:

1 “SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT
2 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 sub-*
8 *chapter:*

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 the*
14 *House of Representatives;*

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

17 “(D) *the Committee on Commerce, Science,*
18 *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, and*
24 *Technology of the House of Representatives;*

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 United
8 States; and

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

11 “(2) AWARDÉE.—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 de-
21 scribed 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 an*
2 *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’ means*
7 *a prime contractor of an agency or a subcontractor*
8 *of a prime contractor of an agency that creates, col-*
9 *lects, stores, processes, maintains, or transmits Fed-*
10 *eral 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, disclosed,*
14 *or disposed of by or for the Federal Government in*
15 *any medium or form.*

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

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

1 “(8) *NATIONWIDE CONSUMER REPORTING AGEN-*
 2 *CY.—The term ‘nationwide consumer reporting agen-*
 3 *cy’ means a consumer reporting agency described in*
 4 *section 603(p) of the Fair Credit Reporting Act (15*
 5 *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 individ-*
 16 *uals is necessary pursuant to subsection (b)(1), re-*
 17 *gardless 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 con-*
 25 *clude that a breach has occurred, the head of the agency,*

1 *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 notification
4 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 per-
8 sonally identifiable information affected by the
9 breach;

10 “(3) contact information of the agency that may
11 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 by
17 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 identi-
21 fiable 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 noti-
11 fication 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 determines
2 there is a significant change in the reasonable basis to con-
3 clude that a breach occurred, a significant change to the
4 determination made under subsection (b)(1), or that it is
5 necessary to update the details of the information provided
6 to potentially affected individuals as described in subsection
7 (c), the agency shall as expeditiously as practicable and
8 without unreasonable delay, and in any case not later than
9 30 days after such a determination, notify each individual
10 who received a notification pursuant to subsection (b) of
11 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 Se-
15 curity 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 head
22 of an agency may submit the report required under
23 paragraph (1) as a component of the report submitted
24 under section 3554(c).

25 “(g) *CONGRESSIONAL REPORTING REQUIREMENTS.*—

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

6 “(2) *REQUIRED NOTICE FROM AGENCIES.*—Sub-
7 ject to paragraph (4), the Director of the Office of
8 Management and Budget shall require the head of an
9 agency affected by a covered breach to expeditiously
10 and not later than 30 days after the date on which
11 the agency discovers the covered breach give notice of
12 the breach, which may be provided electronically, to—

13 “(A) each congressional committee described
14 in section 3554(c)(1); and

15 “(B) the Committee on the Judiciary of the
16 Senate and the Committee on the Judiciary of
17 the House of Representatives.

18 “(3) *CONTENTS OF NOTICE.*—Notice of a covered
19 breach provided by the head of an agency pursuant
20 to paragraph (2) shall include, to the extent prac-
21 ticable—

22 “(A) information about the covered breach,
23 including a summary of any information about
24 how the covered breach occurred known by the
25 agency as of the date of the notice;

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

6 “(C) a description of any circumstances ne-
7 cessitating a delay in providing notice to indi-
8 viduals affected by the covered breach in accord-
9 ance with subsection (d); and

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

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

17 “(A) the majority and minority leaders of
18 the Senate;

19 “(B) the Speaker and minority leader of the
20 House of Representatives;

21 “(C) the appropriations committees of Con-
22 gress;

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

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

3 “(F) the Committee on Oversight and Ac-
4 countability of the House of Representatives; and

5 “(G) the Permanent Select Committee on
6 Intelligence of the House of Representatives.

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

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

12 “(1) limit—

13 “(A) the authority of the Director to issue
14 guidance relating to notifications of, or the head
15 of an agency to notify individuals potentially af-
16 fected by, breaches that are not determined to be
17 covered breaches or major incidents;

18 “(B) the authority of the Director to issue
19 guidance relating to notifications and reporting
20 of breaches, covered breaches, or major incidents;

21 “(C) the authority of the head of an agency
22 to provide more information than required under
23 subsection (b) when notifying individuals poten-
24 tially affected by a breach;

1 “(D) the timing of incident reporting or the
2 types of information included in incident reports
3 provided, pursuant to this subchapter, to—

4 “(i) the Director;

5 “(ii) the National Cyber Director;

6 “(iii) the Director of the Cybersecurity
7 and Infrastructure Security Agency; or

8 “(iv) any other agency;

9 “(E) the authority of the head of an agency
10 to provide information to Congress about agency
11 breaches, including—

12 “(i) breaches that are not covered
13 breaches; and

14 “(ii) additional information beyond
15 the information described in subsection
16 (g)(3); or

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

19 “(2) limit or supersede any existing privacy pro-
20 tectons in existing law.

21 **“§ 3593. Congressional and executive branch reports**
22 **on major incidents**

23 “(a) *APPROPRIATE CONGRESSIONAL ENTITIES.*—*In*
24 *this section, the term ‘appropriate congressional entities’*
25 *means—*

1 “(1) *the majority and minority leaders of the*
2 *Senate;*

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

5 “(3) *the Committee on Homeland Security and*
6 *Governmental Affairs of the Senate;*

7 “(4) *the Committee on Commerce, Science, and*
8 *Transportation of the Senate;*

9 “(5) *the Committee on Oversight and Account-*
10 *ability of the House of Representatives;*

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

13 “(7) *the Committee on Science, Space, and Tech-*
14 *nology of the House of Representatives; and*

15 “(8) *the appropriate authorization and appro-*
16 *propriations committees of Congress.*

17 “(b) *INITIAL NOTIFICATION.—*

18 “(1) *IN GENERAL.—Not later than 72 hours after*
19 *an agency has a reasonable basis to conclude that a*
20 *major incident occurred, the head of the agency im-*
21 *pacted by the major incident shall submit to the ap-*
22 *propriate reporting entities a written notification,*
23 *which may be submitted electronically and include 1*
24 *or more annexes that contain classified or other sen-*
25 *sitive information, as appropriate.*

1 “(2) *CONTENTS.*—A notification required under
2 *paragraph (1) with respect to a major incident shall*
3 *include the following, based on information available*
4 *to agency officials as of the date on which the agency*
5 *submits the notification:*

6 “(A) *A summary of the information avail-*
7 *able about the major incident, including how the*
8 *major incident occurred and the threat causing*
9 *the major incident.*

10 “(B) *If applicable, information relating to*
11 *any breach associated with the major incident,*
12 *regardless of whether—*

13 “(i) *the breach was the reason the inci-*
14 *dent was determined to be a major incident;*
15 *and*

16 “(ii) *head of the agency determined it*
17 *was appropriate to provide notification to*
18 *potentially impacted individuals pursuant*
19 *to section 3592(b)(1).*

20 “(C) *A preliminary assessment of the im-*
21 *pacts to—*

22 “(i) *the agency;*

23 “(ii) *the Federal Government;*

1 “(iii) the national security, foreign re-
2 lations, homeland security, and economic
3 security of the United States; and

4 “(iv) the civil liberties, public con-
5 fidence, privacy, and public health and
6 safety of the people of the United States.

7 “(D) If applicable, whether any ransom has
8 been demanded or paid, or is expected to be
9 paid, by any entity operating a Federal infor-
10 mation system or with access to Federal infor-
11 mation or a Federal information system, includ-
12 ing, as available, the name of the entity demand-
13 ing ransom, the date of the demand, and the
14 amount and type of currency demanded, unless
15 disclosure of such information will disrupt an
16 active Federal law enforcement or national secu-
17 rity operation.

18 “(c) SUPPLEMENTAL UPDATE.—Within a reasonable
19 amount of time, but not later than 30 days after the date
20 on which the head of an agency submits a written notifica-
21 tion under subsection (b), the head of the agency shall pro-
22 vide to the appropriate congressional entities an unclassi-
23 fied and written update, which may include 1 or more an-
24 nexes that contain classified or other sensitive information,
25 as appropriate, on the major incident, based on informa-

1 *tion available to agency officials as of the date on which*
2 *the agency provides the update, on—*

3 “(1) *system vulnerabilities relating to the major*
4 *incident, where applicable, means by which the major*
5 *incident occurred, the threat causing the major inci-*
6 *dent, where applicable, and impacts of the major inci-*
7 *dent to—*

8 “(A) *the agency;*

9 “(B) *other Federal agencies, Congress, or*
10 *the judicial branch;*

11 “(C) *the national security, foreign relations,*
12 *homeland security, or economic security of the*
13 *United States; or*

14 “(D) *the civil liberties, public confidence,*
15 *privacy, or public health and safety of the people*
16 *of the United States;*

17 “(2) *the status of compliance of the affected Fed-*
18 *eral information system with applicable security re-*
19 *quirements at the time of the major incident;*

20 “(3) *if the major incident involved a breach, a*
21 *description of the affected information, an estimate of*
22 *the number of individuals potentially impacted, and*
23 *any assessment to the risk of harm to such individ-*
24 *uals;*

1 “(4) an update to the assessment of the risk to
2 agency operations, or to impacts on other agency or
3 non-Federal entity operations, affected by the major
4 incident;

5 “(5) the detection, response, and remediation ac-
6 tions of the agency, including any support provided
7 by the Cybersecurity and Infrastructure Security
8 Agency under section 3594(d), if applicable;

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

12 “(7) as appropriate and available, recommenda-
13 tions for mitigating future similar incidents, includ-
14 ing recommendations from any non-Federal entity
15 impacted by or supporting the remediation of the
16 major incident.

17 “(d) *ADDITIONAL UPDATE.*—If the head of an agency,
18 the Director, or the National Cyber Director determines that
19 there is any significant change in the understanding of the
20 scope, scale, or consequence of a major incident for which
21 the head of the agency submitted a written notification and
22 update under subsections (b) and (c), the head of the agency
23 shall submit to the appropriate congressional entities a
24 written update that includes information relating to the
25 change in understanding.

1 “(e) *BIENNIAL REPORT.*—Each agency shall submit as
2 part of the biennial report required under section
3 3554(c)(1) a description of each major incident that oc-
4 curred during the 2-year period preceding the date on which
5 the biennial report is submitted.

6 “(f) *REPORT DELIVERY.*—

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

9 “(A) shall be submitted in an electronic for-
10 mat; and

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

12 “(2) *CLASSIFICATION STATUS.*—Any written no-
13 tification or update required to be submitted under
14 this section—

15 “(A) shall be—

16 “(i) unclassified; and

17 “(ii) submitted through unclassified
18 electronic means pursuant to paragraph
19 (1)(A); and

20 “(B) may include classified annexes, as ap-
21 propriate.

22 “(g) *REPORT CONSISTENCY.*—To achieve consistent
23 and coherent agency reporting to Congress, the National
24 Cyber Director, in coordination with the Director, shall—

1 “(1) provide recommendations to agencies on for-
2 matting and the contents of information to be in-
3 cluded in the reports required under this section, in-
4 cluding recommendations for consistent formats for
5 presenting any associated metrics; and

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

9 “(A) include, at a minimum—

10 “(i) the full contents of the written no-
11 tification or update;

12 “(ii) the identity of the reporting agen-
13 cy; and

14 “(iii) the date of submission; and

15 “(iv) a list of the recipient congres-
16 sional entities; and

17 “(B) be made available upon request to the
18 majority and minority leaders of the Senate, the
19 Speaker and minority leader of the House of
20 Representatives, the Committee on Homeland Se-
21 curity and Governmental Affairs of the Senate,
22 and the Committee on Oversight and Account-
23 ability of the House of Representatives.

24 “(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL
25 REPORTING EXEMPTION.—With respect to a major incident

1 *that occurs exclusively on a national security system, the*
2 *head of the affected agency shall submit the notifications*
3 *and reports required to be submitted to Congress under this*
4 *section only to—*

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

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

9 “(3) *the appropriations committees of Congress;*

10 “(4) *the appropriate authorization committees of*
11 *Congress;*

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

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

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

18 “(8) *the Permanent Select Committee on Intel-*
19 *ligence of the House of Representatives.*

20 “(i) *MAJOR INCIDENTS INCLUDING BREACHES.—If a*
21 *major incident constitutes a covered breach, as defined in*
22 *section 3592(a), information on the covered breach required*
23 *to be submitted to Congress pursuant to section 3592(g)*
24 *may—*

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

3 “(2) be reported to Congress under the process es-
4 tablished under section 3592(g).

5 “(j) *RULE OF CONSTRUCTION.*—Nothing in this sec-
6 tion shall be construed to—

7 “(1) limit—

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

10 “(B) Congress from requesting additional
11 information from agencies through reports, brief-
12 ings, or other means; and

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

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

17 “**§ 3594. Government information sharing and inci-**
18 **dent response**

19 “(a) *IN GENERAL.*—

20 “(1) *INCIDENT SHARING.*—Subject to paragraph
21 (4) and subsection (b), and in accordance with the
22 applicable requirements pursuant to section
23 3553(b)(2)(A) for reporting to the Federal informa-
24 tion security incident center established under section
25 3556, the head of each agency shall provide to the Cy-

1 *bersecurity and Infrastructure Security Agency infor-*
2 *mation relating to any incident affecting the agency,*
3 *whether the information is obtained by the Federal*
4 *Government directly or indirectly.*

5 “(2) *CONTENTS.*—*A provision of information re-*
6 *lating to an incident made by the head of an agency*
7 *under paragraph (1) shall include, at a minimum—*

8 “(A) *a full description of the incident, in-*
9 *cluding—*

10 “(i) *all indicators of compromise and*
11 *tactics, techniques, and procedures;*

12 “(ii) *an indicator of how the intruder*
13 *gained initial access, accessed agency data*
14 *or systems, and undertook additional ac-*
15 *tions on the network of the agency;*

16 “(iii) *information that would support*
17 *enabling defensive measures; and*

18 “(iv) *other information that may assist*
19 *in identifying other victims;*

20 “(B) *information to help prevent similar*
21 *incidents, such as information about relevant*
22 *safeguards in place when the incident occurred*
23 *and the effectiveness of those safeguards; and*

24 “(C) *information to aid in incident re-*
25 *sponse, such as—*

1 “(i) a description of the affected sys-
2 tems or networks;

3 “(ii) the estimated dates of when the
4 incident occurred; and

5 “(iii) information that could reason-
6 ably help identify any malicious actor that
7 may have conducted or caused the incident,
8 subject to appropriate privacy protections.

9 “(3) INFORMATION SHARING.—The Director of
10 the Cybersecurity and Infrastructure Security Agency
11 shall—

12 “(A) make incident information provided
13 under paragraph (1) available to the Director
14 and the National Cyber Director;

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

17 “(i) the head of any agency that may
18 be—

19 “(I) impacted by the incident;

20 “(II) particularly susceptible to
21 the incident; or

22 “(III) similarly targeted by the
23 incident; and

1 “(ii) appropriate Federal law enforce-
2 ment agencies to facilitate any necessary
3 threat response activities, as requested;

4 “(C) coordinate any necessary information
5 sharing efforts relating to a major incident with
6 the private sector; and

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

9 “(4) NATIONAL SECURITY SYSTEMS EXEMP-
10 TION.—

11 “(A) IN GENERAL.—Notwithstanding para-
12 graphs (1) and (3), each agency operating or ex-
13 ercising control of a national security system
14 shall share information about an incident that
15 occurs exclusively on a national security system
16 with the Secretary of Defense, the Director, the
17 National Cyber Director, and the Director of the
18 Cybersecurity and Infrastructure Security Agen-
19 cy to the extent consistent with standards and
20 guidelines for national security systems issued in
21 accordance with law and as directed by the
22 President.

23 “(B) PROTECTIONS.—Any information
24 sharing and handling of information under this
25 paragraph shall be appropriately protected con-

1 *sistent with procedures authorized for the protec-*
2 *tion of sensitive sources and methods or by pro-*
3 *cedures established for information that have*
4 *been specifically authorized under criteria estab-*
5 *lished by an Executive order or an Act of Con-*
6 *gress to be kept classified in the interest of na-*
7 *tional defense or foreign policy.*

8 “(b) *AUTOMATION.*—*In providing information and se-*
9 *lecting a method to provide information under subsection*
10 *(a), the head of each agency shall implement subsection*
11 *(a)(1) in a manner that provides such information to the*
12 *Cybersecurity and Infrastructure Security Agency in an*
13 *automated and machine-readable format, to the greatest ex-*
14 *tent practicable.*

15 “(c) *INCIDENT RESPONSE.*—*Each agency that has a*
16 *reasonable basis to suspect or conclude that a major inci-*
17 *dent occurred involving Federal information in electronic*
18 *medium or form that does not exclusively involve a national*
19 *security system shall coordinate with—*

20 “(1) *the Cybersecurity and Infrastructure Secu-*
21 *urity Agency to facilitate asset response activities and*
22 *provide recommendations for mitigating future inci-*
23 *dents; and*

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

4 **“§ 3595. Responsibilities of contractors and awardees**

5 “(a) NOTIFICATION.—

6 “(1) IN GENERAL.—Any contractor or awardee
7 of an agency shall provide written notification to the
8 agency if the contractor or awardee has a reasonable
9 basis to conclude that—

10 “(A) an incident or breach has occurred
11 with respect to Federal information the con-
12 tractor or awardee collected, used, or maintained
13 on behalf of an agency;

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

18 “(C) a component of any Federal informa-
19 tion system operated, managed, or maintained
20 by a contractor or awardee contains a security
21 vulnerability, including a supply chain com-
22 promise or an identified software or hardware
23 vulnerability, for which there is reliable evidence
24 of a successful exploitation of the vulnerability

1 *by an actor without authorization of the Federal*
2 *information system owner; or*

3 “(D) *the contractor or awardee has received*
4 *from the agency personally identifiable informa-*
5 *tion or personal health information that is be-*
6 *yond the scope of the contract or agreement with*
7 *the agency that the contractor or awardee is not*
8 *authorized to receive.*

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

24 “(3) *PROCEDURES.—*

1 “(A) *SHARING WITH CISA.*—As soon as
2 *practicable following a notification of an inci-*
3 *dent or vulnerability to an agency by a con-*
4 *tractor or awardee under paragraph (1), the*
5 *head of the agency shall provide, pursuant to sec-*
6 *tion 3594, information about the incident or vul-*
7 *nerability to the Director of the Cybersecurity*
8 *and Infrastructure Security Agency.*

9 “(B) *TIMING OF NOTIFICATIONS.*—Unless a
10 *different time for notification is specified in a*
11 *contract, grant, cooperative agreement, or other*
12 *transaction agreement, a contractor or awardee*
13 *shall—*

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

20 “(ii) *make a notification required*
21 *under paragraph (2) within a reasonable*
22 *time, but not later than 90 days after the*
23 *date on which the contractor or awardee has*
24 *reasonable basis to suspect or conclude that*

1 *the criteria under paragraph (2) have been*
2 *met.*

3 “(C) *PROCEDURES.*—*Following a notifica-*
4 *tion of a breach or incident to an agency by a*
5 *contractor or awardee under paragraph (1), the*
6 *head of the agency, in consultation with the con-*
7 *tractor or awardee, shall carry out the applicable*
8 *requirements under sections 3592, 3593, and*
9 *3594 with respect to the breach or incident.*

10 “(D) *RULE OF CONSTRUCTION.*—*Nothing in*
11 *subparagraph (B) shall be construed to allow the*
12 *negation of the requirements to notify*
13 *vulnerabilities under paragraph (1) or (2)*
14 *through a contract, grant, cooperative agreement,*
15 *or other transaction agreement.*

16 “(4) *GUIDANCE.*—*The Director shall issue guid-*
17 *ance as soon as practicable to agencies relating to the*
18 *scope of vulnerabilities to be included in required no-*
19 *tifications under paragraph (2), such as the min-*
20 *imum severity or minimum risk level of a vulner-*
21 *ability included in required notifications, whether*
22 *vulnerabilities that are already publicly disclosed*
23 *must be reported, or likely cybersecurity impact to*
24 *Federal information systems.*

25 “(b) *REGULATIONS; MODIFICATIONS.*—

1 “(1) *IN GENERAL.*—Not later than 2 years after
2 the date of enactment of the Federal Information Se-
3 curity Modernization Act of 2024—

4 “(A) *the Federal Acquisition Regulatory*
5 *Council shall promulgate regulations, as appro-*
6 *priate, relating to the responsibilities of contrac-*
7 *tors and recipients of other transaction agree-*
8 *ments and cooperative agreements to comply*
9 *with this section; and*

10 “(B) *the Office of Federal Financial Man-*
11 *agement shall promulgate regulations under title*
12 *2, Code of Federal Regulations, as appropriate,*
13 *relating to the responsibilities of grantees to com-*
14 *ply with this section.*

15 “(2) *IMPLEMENTATION.*—Not later than 1 year
16 after the date on which the Federal Acquisition Regu-
17 latory Council and the Office of Federal Financial
18 Management promulgates regulations under para-
19 graph (1), the head of each agency shall implement
20 policies and procedures, as appropriate, necessary to
21 implement those regulations.

22 “(3) *CONGRESSIONAL NOTIFICATION.*—

23 “(A) *IN GENERAL.*—The head of each agen-
24 cy head shall notify the Director upon imple-
25 mentation of policies and procedures necessary to

1 *implement the regulations promulgated under*
2 *paragraph (1).*

3 “(B) *OMB NOTIFICATION.*— *Not later than*
4 *30 days after the date described in paragraph*
5 *(2), the Director shall notify the Committee on*
6 *Homeland Security and Governmental Affairs of*
7 *the Senate and the Committees on Oversight and*
8 *Accountability and Homeland Security of the*
9 *House of Representatives on the status of the im-*
10 *plementation by each agency of the regulations*
11 *promulgated under paragraph (1).*

12 “(c) *ALLOWABLE USE.*—*Information provided to an*
13 *agency pursuant to this section may be disclosed to, re-*
14 *tained by, and used by any agency, component, officer, em-*
15 *ployee, or agent of the Federal Government solely for any*
16 *of the following:*

17 “(1) *A cybersecurity purpose (as defined in sec-*
18 *tion 2200 of the Homeland Security Act of 2002 (6*
19 *U.S.C. 650)).*

20 “(2) *Identifying—*

21 “(A) *a cyber threat (as defined in such sec-*
22 *tion 2200), including the source of the cyber*
23 *threat; or*

24 “(B) *a security vulnerability (as defined in*
25 *such section 2200).*

1 “(3) *Preventing, investigating, disrupting, or*
2 *prosecuting an offense arising out of an incident noti-*
3 *fied to an agency pursuant to this section or any of*
4 *the offenses listed in section 105(d)(5)(A)(v) of the Cy-*
5 *bersecurity Information Sharing Act of 2015 (6*
6 *U.S.C. 1504(d)(5)(A)(v)).*

7 “(d) *HARMONIZATION OF OTHER PRIVATE-SECTOR*
8 *CYBERSECURITY REPORTING OBLIGATIONS.—Any non-*
9 *Federal entity required to report an incident under section*
10 *2242 of the Homeland Security Act of 2002 (6 U.S.C. 681b)*
11 *may submit as part of the written notification requirements*
12 *in this section all information required by such section 2242*
13 *to the agency of which the entity is a contractor or recipient*
14 *of Federal financial assistance, or with which the entity*
15 *holds an other transaction agreement or cooperative agree-*
16 *ment, within the deadline specified in subsection*
17 *(a)(3)(B)(1). If such submission is completed, the non-Fed-*
18 *eral entity shall not be required to subsequently report the*
19 *same incident under the requirements of such section 2242.*
20 *Any incident information shared under this subsection shall*
21 *be shared with the Director of the Cybersecurity and Infra-*
22 *structure Security Agency pursuant to subsection (a)(3)(A).*

23 “(e) *NATIONAL SECURITY SYSTEMS EXEMPTION.—*
24 *Notwithstanding any other provision of this section, a con-*
25 *tractor or awardee of an agency that would be required to*

1 *report an incident or vulnerability pursuant to this section*
2 *that occurs exclusively on a national security system*
3 *shall—*

4 “(1) *report the incident or vulnerability to the*
5 *head of the agency and the Secretary of Defense; and*

6 “(2) *comply with applicable laws and policies*
7 *relating to national security systems.*

8 **“§ 3596. Training**

9 “(a) *COVERED INDIVIDUAL DEFINED.—In this section,*
10 *the term ‘covered individual’ means an individual who ob-*
11 *tains access to a Federal information system because of the*
12 *status of the individual as—*

13 “(1) *an employee, contractor, awardee, volunteer,*
14 *or intern of an agency; or*

15 “(2) *an employee of a contractor or awardee of*
16 *an agency.*

17 “(b) *BEST PRACTICES AND CONSISTENCY.—The Direc-*
18 *tor of the Cybersecurity and Infrastructure Security Agen-*
19 *cy, in consultation with the Director, the National Cyber*
20 *Director, and the Director of the National Institute of*
21 *Standards and Technology, shall consolidate best practices*
22 *to support consistency across agencies in cybersecurity inci-*
23 *dent response training, including—*

24 “(1) *information to be collected and shared with*
25 *the Cybersecurity and Infrastructure Security Agency*

1 *pursuant to section 3594(a) and processes for sharing*
2 *such information; and*

3 “(2) *appropriate training and qualifications for*
4 *cyber incident responders.*

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

8 “(1) *the internal process of the agency for report-*
9 *ing an incident; and*

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

14 “(d) *INCLUSION IN ANNUAL TRAINING.—The training*
15 *developed under subsection (c) may be included as part of*
16 *an annual privacy, security awareness, or other appro-*
17 *priate training of an agency.*

18 **“§ 3597. Analysis and report on Federal incidents**

19 “(a) *ANALYSIS OF FEDERAL INCIDENTS.—*

20 “(1) *QUANTITATIVE AND QUALITATIVE ANAL-*
21 *YSES.—The Director of the Cybersecurity and Infra-*
22 *structure Security Agency shall perform and, in co-*
23 *ordination with the Director and the National Cyber*
24 *Director, develop, continuous monitoring and quan-*

1 *titative and qualitative analyses of incidents at agen-*
2 *cies, including major incidents, including—*

3 *“(A) the causes of incidents, including—*

4 *“(i) attacker tactics, techniques, and*
5 *procedures; and*

6 *“(ii) system vulnerabilities, including*
7 *zero days, unpatched systems, and informa-*
8 *tion system misconfigurations;*

9 *“(B) the scope and scale of incidents at*
10 *agencies;*

11 *“(C) common root causes of incidents across*
12 *multiple agencies;*

13 *“(D) agency incident response, recovery,*
14 *and remediation actions and the effectiveness of*
15 *those actions, as applicable;*

16 *“(E) lessons learned and recommendations*
17 *in responding to, recovering from, remediating,*
18 *and mitigating future incidents; and*

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

24 *“(2) AUTOMATED ANALYSIS.—The analyses de-*
25 *veloped under paragraph (1) shall, to the greatest ex-*

1 *tent practicable, use machine-readable data, automa-*
2 *tion, and machine learning processes.*

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

4 *“(A) IN GENERAL.—The Director of the Cy-*
5 *bersecurity and Infrastructure Security Agency*
6 *shall share on an ongoing basis the analyses and*
7 *underlying data required under this subsection*
8 *with agencies, the Director, and the National*
9 *Cyber Director to—*

10 *“(i) improve the understanding of cy-*
11 *bersecurity risk of agencies; and*

12 *“(ii) support the cybersecurity im-*
13 *provement efforts of agencies.*

14 *“(B) FORMAT.—In carrying out subpara-*
15 *graph (A), the Director of the Cybersecurity and*
16 *Infrastructure Security Agency shall share the*
17 *analyses—*

18 *“(i) in human-readable written prod-*
19 *ucts; and*

20 *“(ii) to the greatest extent practicable,*
21 *in machine-readable formats in order to en-*
22 *able automated intake and use by agencies.*

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

1 “(b) *ANNUAL REPORT ON FEDERAL INCIDENTS.*—Not
2 *later than 2 years after the date of enactment of this section,*
3 *and not less frequently than annually thereafter, the Direc-*
4 *tor of the Cybersecurity and Infrastructure Security Agen-*
5 *cy, in consultation with the Director, the National Cyber*
6 *Director and the heads of other agencies, as appropriate,*
7 *shall submit to the appropriate reporting entities a report*
8 *that includes—*

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

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

16 “(A) *a specific analysis of breaches; and*

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

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

22 “(A) *a description of each major incident;*

23 “(B) *the total number of incidents of the*
24 *agency; and*

1 “(C) *an analysis of the agency’s perform-*
2 *ance against the metrics established under sec-*
3 *tion 224(c) of the Cybersecurity Act of 2015 (6*
4 *U.S.C. 1522(c)).*

5 “(c) *PUBLICATION.—*

6 “(1) *IN GENERAL.—The Director of the Cyberse-*
7 *curity and Infrastructure Security Agency shall make*
8 *a version of each report submitted under subsection*
9 *(b) publicly available on the website of the Cybersecu-*
10 *rity and Infrastructure Security Agency during the*
11 *year during which the report is submitted.*

12 “(2) *EXEMPTION.—The publication requirement*
13 *under paragraph (1) shall not apply to a portion of*
14 *a report that contains content that should be protected*
15 *in the interest of national security, as determined by*
16 *the Director, the Director of the Cybersecurity and In-*
17 *frastructure Security Agency, or the National Cyber*
18 *Director.*

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

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

1 “(A) *COMPILATION.*—Subject to subpara-
2 graph (B), in making a report publicly available
3 under paragraph (1), the Director of the Cyberse-
4 curity and Infrastructure Security Agency shall
5 sufficiently compile information so that no spe-
6 cific incident of an agency can be identified.

7 “(B) *EXCEPTION.*—The Director of the Cy-
8 bersecurity and Infrastructure Security Agency
9 may include information that enables a specific
10 incident of an agency to be identified in a pub-
11 licly available report—

12 “(i) with the concurrence of the Direc-
13 tor and the National Cyber Director;

14 “(ii) in consultation with the impacted
15 agency, which may, as appropriate, consult
16 with any non-Federal entity impacted by or
17 supporting the remediation of such incident;
18 and

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

21 “(d) *INFORMATION PROVIDED BY AGENCIES.*—

22 “(1) *IN GENERAL.*—The analysis required under
23 subsection (a) and each report submitted under sub-
24 section (b) shall use information provided by agencies
25 under section 3594(a).

1 “(2) *NONCOMPLIANCE REPORTS.*—*During any*
2 *year during which the head of an agency does not*
3 *provide data for an incident to the Cybersecurity and*
4 *Infrastructure Security Agency in accordance with*
5 *section 3594(a), the head of the agency, in coordina-*
6 *tion with the Director of the Cybersecurity and Infra-*
7 *structure Security Agency and the Director, shall sub-*
8 *mit to the appropriate reporting entities a report that*
9 *includes the information described in subsection (b)*
10 *with respect to the agency.*

11 “(e) *NATIONAL SECURITY SYSTEM REPORTS.*—

12 “(1) *IN GENERAL.*—*Notwithstanding any other*
13 *provision of this section, the Secretary of Defense, in*
14 *consultation with the Director, the National Cyber*
15 *Director, the Director of National Intelligence, and*
16 *the Director of the Cybersecurity and Infrastructure*
17 *Security Agency shall annually submit a report that*
18 *includes the information described in subsection (b)*
19 *with respect to national security systems, to the extent*
20 *that the submission is consistent with standards and*
21 *guidelines for national security systems issued in ac-*
22 *cordance with law and as directed by the President,*
23 *to—*

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

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

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

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

7 “(E) the Committee on Armed Services of
8 the Senate;

9 “(F) the Committee on Appropriations of
10 the Senate;

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

13 “(H) the Committee on Homeland Security
14 of the House of Representatives;

15 “(I) the Permanent Select Committee on In-
16 telligence of the House of Representatives;

17 “(J) the Committee on Armed Services of
18 the House of Representatives; and

19 “(K) the Committee on Appropriations of
20 the House of Representatives.

21 “(2) CLASSIFIED FORM.—A report required
22 under paragraph (1) may be submitted in a classified
23 form.

1 **“§ 3598. Major incident definition**

2 “(a) *IN GENERAL.*—Not later than 1 year after the
3 later of the date of enactment of the Federal Information
4 Security Modernization Act of 2024 and the most recent
5 publication by the Director of guidance to agencies regard-
6 ing major incidents as of the date of enactment of the Fed-
7 eral Information Security Modernization Act of 2024, the
8 Director shall develop, in coordination with the National
9 Cyber Director, and promulgate guidance on the definition
10 of the term ‘major incident’ for the purposes of subchapter
11 II and this subchapter.

12 “(b) *REQUIREMENTS.*—With respect to the guidance
13 issued under subsection (a), the definition of the term
14 ‘major incident’ shall—

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

18 “(A) any incident the head of the agency
19 determines is likely to result in demonstrable
20 harm to—

21 “(i) the national security interests, for-
22 eign relations, homeland security, or eco-
23 nomic security of the United States; or

24 “(ii) the civil liberties, public con-
25 fidence, privacy, or public health and safety
26 of the people of the United States;

1 “(B) any incident the head of the agency
2 determines likely to result in an inability or sub-
3 stantial disruption for the agency, a component
4 of the agency, or the Federal Government, to pro-
5 vide 1 or more critical services;

6 “(C) any incident the head of the agency
7 determines substantially disrupts or substan-
8 tially degrades the operations of a high value
9 asset owned or operated by the agency;

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

16 “(E) any other type of incident determined
17 appropriate by the Director;

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

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

25 “(B) is enabled by—

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

5 “(ii) the related activities of a common
6 threat actor;

7 “(3) stipulate that, in determining whether an
8 incident constitutes a major incident under the stand-
9 ards described in paragraph (1), the head of the agen-
10 cy shall consult with the National Cyber Director;
11 and

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

16 “(c) *EVALUATION AND UPDATES.*—Not later than 60
17 days after the date on which the Director first promulgates
18 the guidance required under subsection (a), and not less fre-
19 quently than once during the first 90 days of each evenly
20 numbered Congress thereafter, the Director shall provide to
21 the Committee on Homeland Security and Governmental
22 Affairs of the Senate and the Committees on Oversight and
23 Accountability and Homeland Security of the House of
24 Representatives a briefing that includes—

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

3 “(2) an evaluation of any necessary updates to
4 the definition of the term ‘major incident’ included in
5 the guidance; and

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

8 (2) *CLERICAL AMENDMENT.*—The table of sec-
9 tions for chapter 35 of title 44, United States Code,
10 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.”.

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

12 (a) *MODERNIZING GOVERNMENT TECHNOLOGY.*—Sub-
13 title G of title X of division A of the National Defense Au-
14 thorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note)
15 is amended in section 1078—

16 (1) by striking subsection (a) and inserting the
17 following:

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

19 “(1) *AGENCY.*—The term ‘agency’ has the mean-
20 ing given the term in section 551 of title 5, United
21 States Code.

1 “(2) *HIGH VALUE ASSET*.—The term ‘high value
2 asset’ has the meaning given the term in section 3552
3 of title 44, United States Code.”;

4 (2) in subsection (b), by adding at the end the
5 following:

6 “(8) *PROPOSAL EVALUATION*.—The Director
7 shall—

8 “(A) give consideration for the use of
9 amounts in the Fund to improve the security of
10 high value assets; and

11 “(B) require that any proposal for the use
12 of amounts in the Fund includes, as appro-
13 priate, and which may be incorporated into oth-
14 erwise required project proposal documenta-
15 tion—

16 “(i) cybersecurity risk management
17 considerations; and

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

20 and

21 (3) in subsection (c)—

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

25 (B) in paragraph (5)—

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

3 (ii) in subparagraph (B), by striking
4 the period at the end and inserting “; and”;
5 and

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

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

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

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

17 (1) in section 11302—

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

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

4 (2) in section 11303(b)(2)(B)—

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

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

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

10 “(iii) whether the function should be
11 performed by a shared service offered by an-
12 other executive agency;”.

13 (c) *SUBCHAPTER II.*—Subchapter II of chapter 113 of
14 subtitle III of title 40, United States Code, is amended—

15 (1) in section 11312(a), by inserting “, including
16 security risks” after “managing the risks”;

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

20 (3) in section 11317, by inserting “security,” be-
21 fore “or schedule”; and

22 (4) in section 11319(b)(1), in the paragraph
23 heading, by striking “CIOS” and inserting “CHIEF IN-
24 FORMATION OFFICERS”.

1 **SEC. 5. ACTIONS TO ENHANCE FEDERAL INCIDENT TRANS-**
2 **PARENCY.**

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

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

9 (A) *develop a plan for the development,*
10 *using systems in place on the date of enactment*
11 *of this Act, of the analysis required under section*
12 *3597(a) of title 44, United States Code, as added*
13 *by this Act, and the report required under sub-*
14 *section (b) of that section that includes—*

15 (i) *a description of any challenges the*
16 *Director of the Cybersecurity and Infra-*
17 *structure Security Agency anticipates en-*
18 *countering; and*

19 (ii) *the use of automation and ma-*
20 *chine-readable formats for collecting, com-*
21 *piling, monitoring, and analyzing data;*
22 *and*

23 (B) *provide to the appropriate congressional*
24 *committees a briefing on the plan developed*
25 *under subparagraph (A).*

1 (2) *BRIEFING.*—*Not later than 1 year after the*
2 *date of enactment of this Act, the Director of the Cy-*
3 *bersecurity and Infrastructure Security Agency shall*
4 *provide to the appropriate congressional committees a*
5 *briefing on—*

6 (A) *the execution of the plan required under*
7 *paragraph (1)(A); and*

8 (B) *the development of the report required*
9 *under section 3597(b) of title 44, United States*
10 *Code, as added by this Act.*

11 (b) *RESPONSIBILITIES OF THE DIRECTOR OF THE OF-*
12 *FICE OF MANAGEMENT AND BUDGET.*—

13 (1) *UPDATING FISMA 2014.*—*Section 2 of the Fed-*
14 *eral Information Security Modernization Act of 2014*
15 *(Public Law 113–283; 128 Stat. 3073) is amended—*

16 (A) *by striking subsections (b) and (d); and*

17 (B) *by redesignating subsections (c), (e),*
18 *and (f) as subsections (b), (c), and (d), respec-*
19 *tively.*

20 (2) *INCIDENT DATA SHARING.*—

21 (A) *IN GENERAL.*—*The Director, in coordi-*
22 *nation with the Director of the Cybersecurity*
23 *and Infrastructure Security Agency, shall de-*
24 *velop, and as appropriate update, guidance, on*
25 *the content, timeliness, and format of the infor-*

1 *mation provided by agencies under section*
2 *3594(a) of title 44, United States Code, as added*
3 *by this Act.*

4 (B) *REQUIREMENTS.—The guidance devel-*
5 *oped under subparagraph (A) shall—*

6 (i) *enable the efficient development*
7 *of—*

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

12 (II) *the report on Federal inci-*
13 *dents required under section 3597(b) of*
14 *title 44, United States Code, as added*
15 *by this Act; and*

16 (ii) *include requirements for the time-*
17 *liness of data production.*

18 (C) *AUTOMATION.—The Director, in coordi-*
19 *nation with the Director of the Cybersecurity*
20 *and Infrastructure Security Agency, shall pro-*
21 *mote, as feasible, the use of automation and ma-*
22 *chine-readable data for data sharing under sec-*
23 *tion 3594(a) of title 44, United States Code, as*
24 *added by this Act.*

25 (3) *CONTRACTOR AND AWARDEE GUIDANCE.—*

1 (A) *IN GENERAL.*—Not later than 1 year
2 after the date of enactment of this Act, the Direc-
3 tor shall issue guidance to agencies on how to
4 deconflict, to the greatest extent practicable, ex-
5 isting regulations, policies, and procedures relat-
6 ing to the responsibilities of contractors and
7 awardees established under section 3595 of title
8 44, United States Code, as added by this Act.

9 (B) *EXISTING PROCESSES.*—To the greatest
10 extent practicable, the guidance issued under
11 subparagraph (A) shall allow contractors and
12 awardees to use existing processes for notifying
13 agencies of incidents involving information of
14 the Federal Government.

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

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

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

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

23 “(13) to another agency, to the extent necessary,
24 to assist the recipient agency in responding to an in-
25 cident (as defined in section 3552 of title 44) or

1 breach (as defined in section 3591 of title 44) or to
2 fulfill the information sharing requirements under
3 section 3594 of title 44.”.

4 **SEC. 6. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SEC-**
5 **TOR ENTITIES IMPACTED BY INCIDENTS.**

6 (a) *DEFINITIONS.*—*In this section:*

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

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

15 (b) *GUIDANCE ON NOTIFICATION OF REPORTING ENTI-*
16 *TIES.*—*Not later than 1 year after the date of enactment*
17 *of this Act, the Director shall develop, in consultation with*
18 *the National Cyber Director, and issue guidance requiring*
19 *the head of each agency to notify a reporting entity in an*
20 *appropriate and timely manner, and take into consider-*
21 *ation the need to coordinate with Sector Risk Management*
22 *Agencies (as defined in section 2200 of the Homeland Secu-*
23 *rity Act of 2002 (6 U.S.C. 650)), as appropriate, of an inci-*
24 *dent at the agency that is likely to substantially affect—*

1 (1) *the confidentiality or integrity of sensitive*
2 *information submitted by the reporting entity to the*
3 *agency pursuant to a statutory or regulatory require-*
4 *ment; or*

5 (2) *any information system (as defined in sec-*
6 *tion 3502 of title 44, United States Code) used in the*
7 *transmission or storage of the sensitive information*
8 *described in paragraph (1).*

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

10 (a) *IN GENERAL.*—*Subchapter II of chapter 35 of title*
11 *44, United States Code, is amended by adding at the end*
12 *the following:*

13 **“§ 3559A. Federal penetration testing**

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

17 “(1) *requires agencies to perform penetration*
18 *testing on information systems, as appropriate, in-*
19 *cluding on high value assets;*

20 “(2) *provides policies governing the development*
21 *of—*

22 “(A) *rules of engagement for using penetra-*
23 *tion testing; and*

1 “(B) procedures to use the results of pene-
2 tration testing to improve the cybersecurity and
3 risk management of the agency;

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

6 “(4) in no manner restricts the authority of the
7 Secretary of Homeland Security or the Director of the
8 Cybersecurity and Infrastructure Agency to conduct
9 threat hunting pursuant to section 3553, or penetra-
10 tion testing under this chapter.

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

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

17 “(1) the Secretary of Defense in the case of a sys-
18 tem described in section 3553(e)(2); and

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

21 (b) *EXISTING GUIDANCE.—*

22 (1) *IN GENERAL.—Compliance with guidance*
23 *issued by the Director relating to penetration testing*
24 *before the date of enactment of this Act shall be*

1 *deemed to be compliant with section 3559A of title 44,*
2 *United States Code, as added by this Act.*

3 (2) *IMMEDIATE NEW GUIDANCE NOT RE-*
4 *QUIRED.—Nothing in section 3559A of title 44,*
5 *United States Code, as added by this Act, shall be*
6 *construed to require the Director to issue new guid-*
7 *ance to agencies relating to penetration testing before*
8 *the date described in paragraph (3).*

9 (3) *GUIDANCE UPDATES.—Notwithstanding*
10 *paragraphs (1) and (2), not later than 2 years after*
11 *the date of enactment of this Act, the Director shall*
12 *review and, as appropriate, update existing guidance*
13 *requiring penetration testing by agencies.*

14 (c) *CLERICAL AMENDMENT.—The table of sections for*
15 *chapter 35 of title 44, United States Code, is amended by*
16 *adding after the item relating to section 3559 the following:*
 “3559A. Federal penetration testing.”.

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

21 *“(9) performing penetration testing that may le-*
22 *verage manual expert analysis to identify threats and*
23 *vulnerabilities within information systems—*

24 *“(A) without consent or authorization from*
25 *agencies; and*

1 “(B) with prior consultation with the head
2 of the agency at least 72 hours in advance of
3 such testing;”.

4 **SEC. 8. VULNERABILITY DISCLOSURE POLICIES.**

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

8 **“§ 3559B. Federal vulnerability disclosure policies**

9 “(a) *PURPOSE; SENSE OF CONGRESS.*—

10 “(1) *PURPOSE.*—The purpose of Federal vulner-
11 ability disclosure policies is to create a mechanism to
12 enable the public to inform agencies of vulnerabilities
13 in Federal information systems.

14 “(2) *SENSE OF CONGRESS.*—It is the sense of
15 Congress that, in implementing the requirements of
16 this section, the Federal Government should take ap-
17 propriate steps to reduce real and perceived burdens
18 in communications between agencies and security re-
19 searchers.

20 “(b) *DEFINITIONS.*—In this section:

21 “(1) *CONTRACTOR.*—The term ‘contractor’ has
22 the meaning given the term in section 3591.

23 “(2) *INTERNET OF THINGS.*—The term ‘internet
24 of things’ has the meaning given the term in Special
25 Publication 800–213 of the National Institute of

1 *Standards and Technology, entitled ‘IoT Device Cy-*
2 *bersecurity Guidance for the Federal Government: Es-*
3 *tablishing IoT Device Cybersecurity Requirements’, or*
4 *any successor document.*

5 “(3) *SECURITY VULNERABILITY.*—*The term ‘se-*
6 *curity vulnerability’ has the meaning given the term*
7 *in section 102 of the Cybersecurity Information Shar-*
8 *ing Act of 2015 (6 U.S.C. 1501).*

9 “(4) *SUBMITTER.*—*The term ‘submitter’ means*
10 *an individual that submits a vulnerability disclosure*
11 *report pursuant to the vulnerability disclosure process*
12 *of an agency.*

13 “(5) *VULNERABILITY DISCLOSURE REPORT.*—*The*
14 *term ‘vulnerability disclosure report’ means a disclo-*
15 *sure of a security vulnerability made to an agency by*
16 *a submitter.*

17 “(c) *GUIDANCE.*—*The Director shall issue guidance to*
18 *agencies that includes—*

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

23 “(2) *direction to not recommend or pursue legal*
24 *action against a submitter or an individual that con-*
25 *ducts a security research activity that—*

1 “(A) represents a good faith effort to iden-
2 tify and report security vulnerabilities in infor-
3 mation systems; or

4 “(B) otherwise represents a good faith effort
5 to follow the vulnerability disclosure policy of the
6 agency developed under subsection (f)(2);

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

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

15 “(5) requirements for providing information to
16 the submitter of a vulnerability disclosure report on
17 the resolution of the vulnerability disclosure report;

18 “(6) a stipulation that the mere identification by
19 a submitter of a security vulnerability, without a sig-
20 nificant compromise of confidentiality, integrity, or
21 availability, does not constitute a major incident; and

22 “(7) the applicability of the guidance to internet
23 of things devices owned or controlled by an agency.

24 “(d) CONSULTATION.—In developing the guidance re-
25 quired under subsection (c)(3), the Director shall consult

1 *with the Director of the Cybersecurity and Infrastructure*
2 *Security Agency.*

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

5 “(1) *provide support to agencies with respect to*
6 *the implementation of the requirements of this section;*

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

10 “(3) *upon a request by an agency, assist the*
11 *agency in the disclosure to vendors of newly identified*
12 *security vulnerabilities in vendor products and serv-*
13 *ices; and*

14 “(4) *as appropriate, implement the requirements*
15 *of this section, in accordance with the authority*
16 *under section 3553(b)(8), as a shared service available*
17 *to agencies.*

18 “(f) *RESPONSIBILITIES OF AGENCIES.*—

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

25 “(A) *an appropriate security contact; and*

1 “(B) the component of the agency that is re-
2 sponsible for the internet accessible services of-
3 fered at the domain.

4 “(2) *VULNERABILITY DISCLOSURE POLICY.*—The
5 head of each agency shall develop and make publicly
6 available a vulnerability disclosure policy for the
7 agency, which shall—

8 “(A) describe—

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

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

15 “(iii) the type of information system
16 testing that is not authorized by the agency;

17 “(iv) the disclosure policy for a con-
18 tractor; and

19 “(v) the disclosure policy of the agency
20 for sensitive information;

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

23 “(i) how the submitter should submit
24 the vulnerability disclosure report; and

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

5 “(C) include any other relevant informa-
6 tion; and

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

11 “(3) IDENTIFIED SECURITY VULNERABILITIES.—
12 The head of each agency shall—

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

15 “(B) commensurate with the risk posed by
16 the security vulnerability, address such security
17 vulnerability using the security vulnerability
18 management process of the agency; and

19 “(C) in accordance with subsection (c)(5),
20 provide information to the submitter of a vulner-
21 ability disclosure report.

22 “(g) EXEMPTIONS.—

23 “(1) IN GENERAL.—The Director and the head of
24 each agency shall carry out this section in a manner

1 *consistent with the protection of national security in-*
2 *formation.*

3 “(2) *LIMITATION.*—*The Director and the head of*
4 *each agency may not publish under subsection (f)(1)*
5 *or include in a vulnerability disclosure policy under*
6 *subsection (f)(2) host names, services, information*
7 *systems, or other information that the Director or the*
8 *head of an agency, in coordination with the Director*
9 *and other appropriate heads of agencies, determines*
10 *would—*

11 “(A) *disrupt a law enforcement investiga-*
12 *tion;*

13 “(B) *endanger national security or intel-*
14 *ligence activities; or*

15 “(C) *impede national defense activities or*
16 *military operations.*

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

19 “(h) *DELEGATION OF AUTHORITY FOR CERTAIN SYS-*
20 *TEMS.*—*The authorities of the Director and the Director of*
21 *the Cybersecurity and Infrastructure Security Agency de-*
22 *scribed in this section shall be delegated—*

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

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

3 “(i) *REVISION OF FEDERAL ACQUISITION REGULA-*
4 *TION.—The Federal Acquisition Regulation shall be revised*
5 *as necessary to implement the provisions under this sec-*
6 *tion.”.*

7 (b) *EXISTING GUIDANCE AND POLICIES.—*

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

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

19 (3) *IMMEDIATE NEW POLICIES NOT REQUIRED.—*
20 *Nothing in section 3559B of title 44, United States*
21 *Code, as added by this title, shall be construed to re-*
22 *quire the head of any agency to issue new policies re-*
23 *lating to vulnerability disclosure policies before the*
24 *issuance of any updated guidance under paragraph*
25 *(4).*

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

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

 “3559B. Federal vulnerability disclosure policies.”.

10 (d) *CONFORMING UPDATE AND REPEAL.*—

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

17 (2) *IMPLEMENTATION AND CONTRACTOR COMPLI-*
18 *ANCE.*—The *IoT Cybersecurity Improvement Act of*
19 *2020 (15 U.S.C. 278g–3a et seq.)* is amended—

20 (A) by striking section 6 (15 U.S.C. 278g–
21 3d); and

22 (B) by striking section 7 (15 U.S.C. 278g–
23 3e).

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

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

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

13 (2) *implementing principles of least privilege in*
14 *administering information security programs;*

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

18 (4) *identifying incidents quickly;*

19 (5) *isolating and removing unauthorized entities*
20 *from agency systems as quickly as practicable, ac-*
21 *counting for intelligence or law enforcement purposes;*
22 *and*

23 (6) *otherwise increasing the resource costs for en-*
24 *tities that cause incidents to be successful.*

25 (b) *PROGRESS REPORT.*—As a part of each report re-
26 *quired to be submitted under section 3553(c) of title 44,*

1 *United States Code, during the period beginning on the date*
2 *that is 4 years after the date of enactment of this Act and*
3 *ending on the date that is 10 years after the date of enact-*
4 *ment of this Act, the Director shall include an update on*
5 *agency implementation of zero trust architecture, which*
6 *shall include—*

7 (1) *a description of steps agencies have com-*
8 *pleted, including progress toward achieving any re-*
9 *quirements issued by the Director, including the*
10 *adoption of any models or reference architecture;*

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

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

16 (c) *CLASSIFIED ANNEX.—Each update required under*
17 *subsection (b) may include 1 or more annexes that contain*
18 *classified or other sensitive information, as appropriate.*

19 (d) *NATIONAL SECURITY SYSTEMS.—*

20 (1) *BRIEFING.—Not later than 1 year after the*
21 *date of enactment of this Act, the Secretary of Defense*
22 *shall provide to the Committee on Homeland Security*
23 *and Governmental Affairs of the Senate, the Com-*
24 *mittee on Oversight and Accountability of the House*
25 *of Representatives, the Committee on Armed Services*

1 *of the Senate, the Committee on Armed Services of the*
2 *House of Representatives, the Select Committee on In-*
3 *telligence of the Senate, and the Permanent Select*
4 *Committee on Intelligence of the House of Representa-*
5 *tives a briefing on the implementation of zero trust*
6 *architecture with respect to national security systems.*

7 (2) *PROGRESS REPORT.*—*Not later than the date*
8 *on which each update is required to be submitted*
9 *under subsection (b), the Secretary of Defense shall*
10 *submit to the congressional committees described in*
11 *paragraph (1) a progress report on the implementa-*
12 *tion of zero trust architecture with respect to national*
13 *security systems.*

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

15 (a) *DEFINITION.*—*In this section, the term “informa-*
16 *tion system” has the meaning given the term in section*
17 *3502 of title 44, United States Code.*

18 (b) *USE OF ARTIFICIAL INTELLIGENCE.*—

19 (1) *IN GENERAL.*—*As appropriate, the Director*
20 *shall issue guidance on the use of artificial intel-*
21 *ligence by agencies to improve the cybersecurity of in-*
22 *formation systems.*

23 (2) *CONSIDERATIONS.*—*The Director and head of*
24 *each agency shall consider the use and capabilities of*

1 *artificial intelligence systems in furtherance of the cy-*
2 *bersecurity of information systems.*

3 (3) *REPORT.*—Not later than 1 year after the
4 *date of enactment of this Act, and annually thereafter*
5 *until the date that is 5 years after the date of enact-*
6 *ment of this Act, the Director shall submit to the ap-*
7 *propriate congressional committees a report on the*
8 *use of artificial intelligence to further the cybersecu-*
9 *rity of information systems.*

10 (c) *COMPTROLLER GENERAL REPORTS.*—

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

19 (2) *STUDY.*—Not later than 2 years after the
20 *date of enactment of this Act, the Comptroller General*
21 *of the United States shall perform a study, and sub-*
22 *mit to the Committees on Homeland Security and*
23 *Governmental Affairs and Commerce, Science, and*
24 *Transportation of the Senate and the Committees on*
25 *Oversight and Accountability, Homeland Security,*

1 *and Science, Space, and Technology of the House of*
2 *Representatives a report, on the use of automation,*
3 *artificial intelligence, including generative artificial*
4 *intelligence, and machine-readable data across the*
5 *Federal Government for cybersecurity purposes, in-*
6 *cluding—*

7 *(A) the automated updating of cybersecurity*
8 *tools, sensors, or processes employed by agencies*
9 *under paragraphs (1), (5)(C), and (8)(B) of sec-*
10 *tion 3554(b) of title 44, United States Code, as*
11 *amended by this Act; and*

12 *(B) to combat social engineering attacks.*

13 **SEC. 11. FEDERAL CYBERSECURITY REQUIREMENTS.**

14 *(a) CODIFYING FEDERAL CYBERSECURITY REQUIRE-*
15 *MENTS IN TITLE 44.—*

16 *(1) AMENDMENT TO FEDERAL CYBERSECURITY*
17 *ENHANCEMENT ACT OF 2015.—Section 225 of the Fed-*
18 *eral Cybersecurity Enhancement Act of 2015 (6*
19 *U.S.C. 1523) is amended by striking subsections (b)*
20 *and (c).*

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

24 *“(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT*
25 *AGENCIES.—*

1 “(1) *IN GENERAL.*—*Consistent with policies,*
2 *standards, guidelines, and directives on information*
3 *security under this subchapter, and except as pro-*
4 *vided under paragraph (3), the head of each agency*
5 *shall—*

6 “(A) *identify sensitive and mission critical*
7 *data stored by the agency consistent with the in-*
8 *ventory required under section 3505(c);*

9 “(B) *assess access controls to the data de-*
10 *scribed in subparagraph (A), the need for readily*
11 *accessible storage of the data, and the need of in-*
12 *dividuals to access the data;*

13 “(C) *encrypt or otherwise render indeci-*
14 *pherable to unauthorized users the data described*
15 *in subparagraph (A) that is stored on or*
16 *transiting agency information systems;*

17 “(D) *implement identity and access man-*
18 *agement systems to ensure the security of Federal*
19 *information systems and protect agency records*
20 *and data from fraud resulting from the mis-*
21 *representation of identity or identity theft, in-*
22 *cluding—*

23 “(i) *a single sign-on trusted identity*
24 *platform for individuals accessing each pub-*
25 *lic website of the agency that requires, at a*

1 *minimum, user authentication and*
2 *verification services consistent with applica-*
3 *ble law and guidance issued by the Director*
4 *of the Office of Management and Budget*
5 *who shall consider any applicable standard*
6 *or guideline developed by the National In-*
7 *stitute of Standards and Technology, which*
8 *may be one developed by the Administrator*
9 *of General Services in consultation with the*
10 *Director of the Office of Management and*
11 *Budget; and*

12 “(ii) *multi-factor authentication, con-*
13 *sistent with guidance issued by the Director*
14 *of the Office of Management and Budget*
15 *who shall consider any applicable standard*
16 *or guideline developed by the National In-*
17 *stitute of Standards and Technology, for—*

18 “(I) *remote access to an informa-*
19 *tion system; and*

20 “(II) *each user account with ele-*
21 *vated privileges on an informa-*
22 *tion system.*

23 “(2) *PROHIBITION.—*

1 “(A) *DEFINITION.*—*In this paragraph, the*
2 *term ‘internet of things’ has the meaning given*
3 *the term in section 3559B.*

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

20 “(3) *EXCEPTIONS.*—

21 “(A) *IN GENERAL.*—*The requirements under*
22 *subparagraphs (A), (B), (C), and (D)(ii) of*
23 *paragraph (1) shall not apply to an information*
24 *system for which the head of the agency, without*
25 *delegation, has—*

1 “(i) certified to the Director with par-
2 ticularity that—

3 “(I) operational requirements ar-
4 ticated in the certification and re-
5 lated to the information system would
6 make it excessively burdensome to im-
7 plement the cybersecurity requirement;

8 “(II) the cybersecurity require-
9 ment is not necessary to secure the in-
10 formation system or agency informa-
11 tion stored on or transiting it; and

12 “(III) the agency has taken all
13 necessary steps to secure the informa-
14 tion system and agency information
15 stored on or transiting it; and

16 “(ii) submitted the certification de-
17 scribed in clause (i) to the appropriate con-
18 gressional committees and the authorizing
19 committees of the agency.

20 “(B) *IDENTITY MANAGEMENT PLATFORM*
21 *WAIVER.*—The head of an agency shall be in
22 compliance with the requirement under para-
23 graph (1)(D)(i) with respect to implementing a
24 single-sign on trusted identity system or plat-
25 form other than one developed by the Adminis-

1 *trator of General Services as described under*
2 *paragraph (1)(D)(i) if the head of the agency—*

3 *“(i) without delegation—*

4 *“(I) has certified to the Director*
5 *that the alternative system or platform,*
6 *including a procured system or plat-*
7 *form, conforms with applicable secu-*
8 *rity and privacy requirements of this*
9 *subchapter and guidance issued by the*
10 *Director, at least 30 days before use of*
11 *the system or platform; or*

12 *“(II) with regard to a system or*
13 *platform in use as of the date of enact-*
14 *ment of this subsection, the head of the*
15 *agency provides such certification to*
16 *the Director within 60 days after the*
17 *date of enactment of this subsection;*

18 *“(ii) has received a written waiver*
19 *from the Director in response to the request*
20 *submitted under clause (i); and*

21 *“(iii) has submitted the certification*
22 *described in clause (i) and the waiver de-*
23 *scribed clause (ii) to the appropriate con-*
24 *gressional committees and the authorizing*
25 *committees of the agency.*

1 “(4) *DURATION OF CERTIFICATION.*—

2 “(A) *IN GENERAL.*—*A certification and cor-*
3 *responding exemption of an agency under para-*
4 *graph (3) shall expire on the date that is 4 years*
5 *after the date on which the head of the agency*
6 *submits the certification under paragraph (3).*

7 “(B) *RENEWAL.*—*Upon the expiration of a*
8 *certification of an agency under paragraph (3),*
9 *the head of the agency may submit an additional*
10 *certification in accordance with that paragraph.*

11 “(5) *PRESUMPTION OF ADEQUACY.*—*A*
12 *FedRAMP authorization issued pursuant to chapter*
13 *36 of title 44 shall be presumed adequate to fulfill the*
14 *requirements under subparagraphs (A) through (C) of*
15 *paragraph (1) with respect to an agency authoriza-*
16 *tion to operate cloud computing products and services*
17 *if such presumption of adequacy does not alter or*
18 *modify—*

19 “(A) *the responsibility of any agency to en-*
20 *sure compliance with this subchapter for any*
21 *cloud computing product or service used by the*
22 *agency; or*

23 “(B) *the authority of the head of any agen-*
24 *cy to make a determination that there is a de-*
25 *monstrable need to include additional security*

1 *controls beyond those included in a FedRAMP*
2 *authorization package for a particular cloud*
3 *computing product or service.*

4 “(6) *RULES OF CONSTRUCTION.—Nothing in this*
5 *subsection shall be construed—*

6 “(A) *to alter the authority of the Secretary,*
7 *the Director, or the Director of the National In-*
8 *stitute of Standards and Technology in imple-*
9 *menting subchapter II of this title;*

10 “(B) *to affect the standards or process of the*
11 *National Institute of Standards and Technology;*

12 “(C) *to affect the requirement under section*
13 *3553(a)(4);*

14 “(D) *to discourage continued improvements*
15 *and advancements in the technology, standards,*
16 *policies, and guidelines used to promote Federal*
17 *information security; or*

18 “(E) *to affect the requirements under sub-*
19 *chapter III.*

20 “(g) *EXCEPTION.—*

21 “(1) *NATIONAL SECURITY SYSTEM REQUIRE-*
22 *MENTS.—The requirements under subsection (f)(1)*
23 *shall not apply to—*

24 “(A) *a national security system; or*

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

3 “(2) *PROHIBITION.*—The prohibition under sub-
4 section (f)(2) shall not apply to—

5 “(A) necessary in the interest of national
6 security;

7 “(B) national security systems; or

8 “(C) a procured internet of things device de-
9 scribed in subsection (f)(2)(B) that the Chief In-
10 formation Officer of an agency determines is—

11 “(i) necessary for research purposes;

12 “(ii) necessary in the interest of na-
13 tional security; or

14 “(iii) secured using alternative and ef-
15 fective methods appropriate to the function
16 of the internet of things device.”.

17 (b) *REPORT ON EXEMPTIONS.*—Section 3554(c)(1) of
18 title 44, United States Code, as amended by this Act, is
19 further amended—

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

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

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

1 “(E) with respect to any exemption from
2 the requirements of subsection (f)(3) that is effec-
3 tive on the date of submission of the report, in-
4 cludes the number of information systems that
5 have received an exemption from those require-
6 ments.”.

7 (c) *GUIDANCE FOR IDENTITY MANAGEMENT SYSTEMS*
8 *USED BY AGENCIES.*—Not later than 1 year after the date
9 of enactment of this Act, the Director of the Office of Man-
10 agement and Budget, in consultation with the Director of
11 the National Institute of Standards and Technology, shall
12 issue, and routinely update thereafter, guidance for agencies
13 to implement identity management systems and a single
14 sign-on trusted identity platform as required under section
15 3554(f)(1)(D)(i) of title 44, United States Code, as amended
16 by this Act, which shall at a minimum, include the fol-
17 lowing:

18 (1) *Requirements for agencies to routinely certify*
19 *that such systems are in compliance with this guid-*
20 *ance.*

21 (2) *Requirements for agencies to routinely verify*
22 *and certify that information stored on or transiting*
23 *through a commercially available product (as defined*
24 *in section 103 of title 41, United States Code) or com-*
25 *mmercial service (as defined in section 103a of title 41,*

1 *United States Code) used to fulfil such requirements*
2 *is appropriately secured in conformity with sub-*
3 *chapter II of chapter 35 of title 44, United States*
4 *Code.*

5 *(3) Address national security concerns and re-*
6 *quirements to ensure the protection of sensitive per-*
7 *sonal records and biometric data of United States*
8 *persons from malign foreign ownership, control, or*
9 *influence and fraud actors.*

10 *(4) Requirements or guidelines to comply with*
11 *section 3 of the 21st Century Idea Act (44 U.S.C.*
12 *3501 note).*

13 *(5) Requirements to prevent discrimination in*
14 *violation of title VI of the Civil Rights Act of 1964*
15 *(42 U.S.C. 2000d et seq.).*

16 *(6) A description of the information necessary to*
17 *be submitted under the exception described in section*
18 *3554(f)(3)(B) of title 44, United States Code, as*
19 *amended by this Act.*

20 *(d) GAO EVALUATION OF TECHNICAL CAPABILITY OF*
21 *IDENTITY MANAGEMENT SYSTEMS AND PLATFORMS.—Not*
22 *less frequently than every 3 years for the next 6 years, the*
23 *Comptroller General shall submit to the appropriate con-*
24 *gressional committees a report on whether the single sign-*
25 *on trusted identity systems and platforms used by agencies*

1 *or the one developed by the General Services Administration*
2 *under section 3554(f)(D)(i) of title 44, United States Code,*
3 *as amended by this Act, adhere to the information security*
4 *requirements of chapter 35 of title 44, United States Code,*
5 *guidance issued under subsection (c), and relevant identity*
6 *management technical standards promulgated by the Na-*
7 *tional Institute of Standards and Technology, as appro-*
8 *priate, including section 504 of the Cybersecurity Enhance-*
9 *ment Act of 2014 (15 U.S.C. 7464).*

10 *(e) DURATION OF CERTIFICATION EFFECTIVE DATE.—*
11 *Paragraph (3) of section 3554(f) of title 44, United States*
12 *Code, as added by this Act, shall take effect on the date*
13 *that is 1 year after the date of enactment of this Act.*

14 *(f) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF*
15 *2015 UPDATE.—Section 222(3)(B) of the Federal Cyberse-*
16 *curity Enhancement Act of 2015 (6 U.S.C. 1521(3)(B)) is*
17 *amended by inserting “and the Committee on Oversight and*
18 *Accountability” before “of the House of Representatives”.*

19 **SEC. 12. FEDERAL CHIEF INFORMATION SECURITY OFFI-**
20 **CER.**

21 *(a) AMENDMENT.—Chapter 36 of title 44, United*
22 *States Code, is amended by adding at the end the following:*

23 **“§ 3617. Federal Chief Information Security Officer**

24 *“(a) ESTABLISHMENT.—There is established a Federal*
25 *Chief Information Security Officer, who shall serve in—*

1 “(1) *the Office of the Federal Chief Information*
2 *Officer of the Office of Management and Budget; and*

3 “(2) *the Office of the National Cyber Director.*

4 “(b) *APPOINTMENT.—The Federal Chief Information*
5 *Security Officer shall be appointed by the President.*

6 “(c) *OMB DUTIES.—The Federal Chief Information*
7 *Security Officer shall report to the Federal Chief Informa-*
8 *tion Officer and assist the Federal Chief Information Offi-*
9 *cer in carrying out—*

10 “(1) *every function under this chapter;*

11 “(2) *every function assigned to the Director*
12 *under title II of the E–Government Act of 2002 (44*
13 *U.S.C. 3501 note; Public Law 107–347);*

14 “(3) *other electronic government initiatives con-*
15 *sistent with other statutes; and*

16 “(4) *other Federal cybersecurity initiatives deter-*
17 *mined by the Federal Chief Information Officer.*

18 “(d) *ADDITIONAL DUTIES.—The Federal Chief Infor-*
19 *mation Security Officer shall—*

20 “(1) *support the Federal Chief Information Offi-*
21 *cer in overseeing and implementing Federal cyberse-*
22 *curity under the E–Government Act of 2002 (Public*
23 *Law 107–347; 116 Stat. 2899) and other relevant*
24 *statutes in a manner consistent with law; and*

1 “(2) *perform every function assigned to the Di-*
2 *rector under sections 1321 through 1328 of title 41,*
3 *United States Code.*

4 “(e) *COORDINATION WITH ONCD.—The Federal Chief*
5 *Information Security Officer shall support initiatives deter-*
6 *mined by the Federal Chief Information Officer necessary*
7 *to coordinate with the Office of the National Cyber Direc-*
8 *tor.”.*

9 (b) *NATIONAL CYBER DIRECTOR DUTIES.—Section*
10 *1752 of the William M. (Mac) Thornberry National Defense*
11 *Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500) is*
12 *amended—*

13 (1) *by redesignating subsection (g) as subsection*
14 *(h); and*

15 (2) *by inserting after subsection (f) the following:*

16 “(g) *SENIOR FEDERAL CYBERSECURITY OFFICER.—*
17 *The Federal Chief Information Security Officer appointed*
18 *by the President under section 3617 of title 44, United*
19 *States Code, shall be a senior official within the Office and*
20 *carry out duties applicable to the protection of information*
21 *technology (as defined in section 11101 of title 40, United*
22 *States Code), including initiatives determined by the Direc-*
23 *tor necessary to coordinate with the Office of the Federal*
24 *Chief Information Officer.”.*

1 (c) *TREATMENT OF INCUMBENT.*—*The individual serv-*
 2 *ing as the Federal Chief Information Security Officer ap-*
 3 *pointed by the President as of the date of enactment of this*
 4 *Act may serve as the Federal Chief Information Security*
 5 *Officer under section 3617 of title 44, United States Code,*
 6 *as added by this Act, beginning on the date of enactment*
 7 *of this Act, without need for a further or additional ap-*
 8 *pointment under such section.*

9 (d) *CLERICAL AMENDMENT.*—*The table of sections for*
 10 *chapter 36 of title 44, United States Code, is amended by*
 11 *adding at the end the following:*

“3617. *Federal Chief Information Security Officer.*”.

12 **SEC. 13. RENAMING OFFICE OF THE FEDERAL CHIEF INFOR-**
 13 **MATION OFFICER.**

14 (a) *DEFINITIONS.*—

15 (1) *IN GENERAL.*—*Section 3601 of title 44,*
 16 *United States Code, is amended—*

17 (A) *by striking paragraph (1); and*

18 (B) *by redesignating paragraphs (2)*
 19 *through (8) as paragraphs (1) through (7), re-*
 20 *spectively.*

21 (2) *CONFORMING AMENDMENTS.*—

22 (A) *TITLE 10.*—*Section 2222(i)(6) of title*
 23 *10, United States Code, is amended by striking*
 24 *“section 3601(4)” and inserting “section 3601”.*

1 (B) NATIONAL SECURITY ACT OF 1947.—Sec-
2 tion 506D(k)(1) of the National Security Act of
3 1947 (50 U.S.C. 3100(k)(1)) is amended by
4 striking “section 3601(4)” and inserting “section
5 3601”.

6 (b) OFFICE OF ELECTRONIC GOVERNMENT.—Section
7 3602 of title 44, United States Code, is amended—

8 (1) in the heading, by striking “**Office of**
9 **Electronic Government**” and inserting “**Office**
10 **of the Federal Chief Information Officer**”;

11 (2) in subsection (a), by striking “Office of Elec-
12 tronic Government” and inserting “Office of the Fed-
13 eral Chief Information Officer”;

14 (3) in subsection (b), by striking “an Adminis-
15 trator” and inserting “a Federal Chief Information
16 Officer”;

17 (4) in subsection (c), in the matter preceding
18 paragraph (1), by striking “The Administrator” and
19 inserting “The Federal Chief Information Officer”;

20 (5) in subsection (d), in the matter preceding
21 paragraph (1), by striking “The Administrator” and
22 inserting “The Federal Chief Information Officer”;

23 (6) in subsection (e), in the matter preceding
24 paragraph (1), by striking “The Administrator” and
25 inserting “The Federal Chief Information Officer”;

1 (7) *in subsection (f)—*

2 (A) *in the matter preceding paragraph (1),*
3 *by striking “the Administrator” and inserting*
4 *“the Federal Chief Information Officer”;*

5 (B) *in paragraph (16), by striking “the Of-*
6 *fice of Electronic Government” and inserting*
7 *“the Office of the Federal Chief Information Offi-*
8 *cer”;* *and*

9 (C) *in paragraph (17), by striking “E-Gov-*
10 *ernment” and inserting “annual”;* *and*

11 (8) *in subsection (g), by striking “the Office of*
12 *Electronic Government” and inserting “the Office of*
13 *the Federal Chief Information Officer”.*

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

16 (1) *in subsection (b)(2), by striking “The Admin-*
17 *istrator of the Office of Electronic Government” and*
18 *inserting “The Federal Chief Information Officer”;*

19 (2) *in subsection (c)(1), by striking “The Admin-*
20 *istrator of the Office of Electronic Government” and*
21 *inserting “The Federal Chief Information Officer”;*
22 *and*

23 (3) *in subsection (f)—*

1 (A) in paragraph (3), by striking “the Ad-
2 ministrators” and inserting “the Federal Chief
3 Information Officer”; and

4 (B) in paragraph (5), by striking “the Ad-
5 ministrators” and inserting “the Federal Chief
6 Information Officer”.

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

9 (1) in subsection (a)(2), by striking “the Admin-
10 istrator of the Office of Electronic Government” and
11 inserting “the Federal Chief Information Officer”;

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

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

18 (e) *PROGRAM TO ENCOURAGE INNOVATIVE SOLUTIONS*
19 *TO ENHANCE ELECTRONIC GOVERNMENT SERVICES AND*
20 *PROCESSES*.—Section 3605 of title 44, United States Code,
21 is amended—

22 (1) in subsection (a), by striking “The Adminis-
23 trator” and inserting “The Federal Chief Information
24 Officer”;

1 (2) *in subsection (b), by striking “, the Adminis-*
2 *trator,” and inserting “, the Federal Chief Informa-*
3 *tion Officer,”; and*

4 (3) *in subsection (c)—*

5 (A) *in paragraph (1)—*

6 (i) *by striking “The Administrator”*
7 *and inserting “The Federal Chief Informa-*
8 *tion Officer”;* and

9 (ii) *by striking “proposals submitted to*
10 *the Administrator” and inserting “pro-*
11 *posals submitted to the Federal Chief Infor-*
12 *mation Officer”;*

13 (B) *in paragraph (2)(B), by striking “the*
14 *Administrator” and inserting “the Federal Chief*
15 *Information Officer”;* and

16 (C) *in paragraph (4), by striking “the Ad-*
17 *ministrator” and inserting “the Federal Chief*
18 *Information Officer”.*

19 (f) *E-GOVERNMENT REPORT.—Section 3606 of title*
20 *44, United States Code, is amended—*

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

23 (2) *in subsection (a), by striking “E-Govern-*
24 *ment” and inserting “annual”;* and

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

3 (g) *TREATMENT OF INCUMBENT.*—*The individual serv-*
4 *ing as the Administrator of the Office of Electronic Govern-*
5 *ment under section 3602 of title 44, United States Code,*
6 *as of the date of enactment of this Act, may continue to*
7 *serve as the Federal Chief Information Officer commencing*
8 *as of that date, without need for a further or additional*
9 *appointment under such section.*

10 (h) *TECHNICAL AND CONFORMING AMENDMENTS.*—
11 *The table of sections for chapter 36 of title 44, United States*
12 *Code, is amended—*

13 (1) *by striking the item relating to section 3602*
14 *and inserting the following:*

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

15 *and*

16 (2) *in the item relating to section 3606, by strik-*
17 *ing “E–Government” and inserting “Annual”.*

18 (i) *REFERENCES.*—

19 (1) *ADMINISTRATOR.*—*Any reference to the Ad-*
20 *ministrator of the Office of Electronic Government in*
21 *any law, regulation, map, document, record, or other*
22 *paper of the United States shall be deemed to be a ref-*
23 *erence to the Federal Chief Information Officer.*

24 (2) *OFFICE OF ELECTRONIC GOVERNMENT.*—*Any*
25 *reference to the Office of Electronic Government in*

1 *any law, regulation, map, document, record, or other*
2 *paper of the United States shall be deemed to be a ref-*
3 *erence to the Office of the Federal Chief Information*
4 *Officer.*

5 **SEC. 14. RULES OF CONSTRUCTION.**

6 (a) *AGENCY ACTIONS.*—*Nothing in this Act, or an*
7 *amendment made by this Act, shall be construed to author-*
8 *ize the head of an agency to take an action that is not au-*
9 *thorized by this Act, an amendment made by this Act, or*
10 *existing law.*

11 (b) *PROTECTION OF RIGHTS.*—*Nothing in this Act, or*
12 *an amendment made by this Act, shall be construed to per-*
13 *mit the violation of the rights of any individual protected*
14 *by the Constitution of the United States, including through*
15 *ensorship of speech protected by the Constitution of the*
16 *United States or unauthorized surveillance.*

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

19 (1) *impinge on the privacy rights of individuals;*

20 *or*

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

Union Calendar No. 790

118TH CONGRESS
2^D SESSION

H. R. 4552

[Report No. 118-939, Part I]

A BILL

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

DECEMBER 19, 2024

Reported from the Committee on Oversight and Accountability with an amendment

DECEMBER 19, 2024

Committees on Science, Space, and Technology; Homeland Security; and Armed Services discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed