

## Calendar No. 674

118TH CONGRESS  
2D SESSION**S. 2251****[Report No. 118–271]**

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

---

## IN THE SENATE OF THE UNITED STATES

JULY 11, 2023

Mr. PETERS (for himself and Mr. HAWLEY) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 9, 2024

Reported by Mr. PETERS, with an amendment

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

**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,*

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

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

5 (b) **TABLE OF CONTENTS.**—The table of contents for  
 6 this Act is as follows:

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

7 **SEC. 2. DEFINITIONS.**

8 In this Act, unless otherwise specified:

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

12 (2) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—  
 13  
 14

1           (A) the Committee on Homeland Security  
2           and Governmental Affairs of the Senate;

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

6           (C) the Committee on Homeland Security  
7           of the House of Representatives.

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

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

14          (5) Director.—The term “Director” means  
15          the Director of the Office of Management and Budg-  
16          et.

17          (6) Federal information system.—The  
18          term “Federal information system” has the meaning  
19          give the term in section 3591 of title 44, United  
20          States Code, as added by this Act.

21          (7) Incident.—The term “incident” has the  
22          meaning given the term in section 3552(b) of title  
23          44, United States Code.

24          (8) National security system.—The term  
25          “national security system” has the meaning given

1 the term in section 3552(b) of title 44, United  
2 States Code.

3 (9) ~~PENETRATION TEST.~~—The term “penetra-  
4 tion test” has the meaning given the term in section  
5 3552(b) of title 44, United States Code, as amended  
6 by this Act.

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

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

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

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

20 (1) in section 3504—

21 (A) in subsection (a)(1)(B)—

22 (i) by striking clause (v) and inserting  
23 the following:

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

1                   (ii) by redesignating clause (vi) as  
2                   clause (vii); and

3                   (iii) by inserting after clause (v) the  
4                   following:

5                   “~~(vi) in consultation with the National~~  
6                   ~~Cyber Director, security of information;~~  
7                   ~~and~~”; and

8                   (B) in subsection (g)—

9                   (i) by redesignating paragraph (2) as  
10                  paragraph (3); and

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

13                  “(1) develop and oversee the implementation of  
14                  policies, principles, standards, and guidelines on pri-  
15                  vaey, confidentiality, disclosure, and sharing of in-  
16                  formation collected or maintained by or for agencies;

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

22                  (2) in section 3505—

23                  (A) by striking the first subsection des-  
24                  ignated as subsection (c);

1           ~~(B)~~ in paragraph ~~(2)~~ of the second sub-  
 2           section designated as subsection ~~(c)~~, by insert-  
 3           ing “an identification of internet accessible in-  
 4           formation systems and” after “an inventory  
 5           under this subsection shall include”;

6           ~~(C)~~ in paragraph ~~(3)~~ of the second sub-  
 7           section designated as subsection ~~(c)~~—

8                     ~~(i)~~ in subparagraph ~~(B)~~—

9                             ~~(I)~~ by inserting “the Director of  
 10                            the Cybersecurity and Infrastructure  
 11                            Security Agency, the National Cyber  
 12                            Director, and” before “the Comp-  
 13                            troller General”; and

14                           ~~(II)~~ by striking “and” at the end;

15                           ~~(ii)~~ in subparagraph ~~(C)(v)~~, by strik-  
 16                            ing the period at the end and inserting “;  
 17                            and”; and

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

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

24                           ~~(A)~~ in subsection ~~(a)(3)~~, by inserting “In  
 25                            carrying out these duties, the Chief Information

1           Officer shall consult, as appropriate, with the  
 2           Chief Data Officer in accordance with the des-  
 3           ignated functions under section 3520(e).” after  
 4           “reduction of information collection burdens on  
 5           the public.”;

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

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

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

11          “(j)(1) Notwithstanding paragraphs (2) and (3) of  
 12          subsection (a), the head of each agency shall designate a  
 13          Chief Privacy Officer with the necessary skills, knowledge,  
 14          and expertise, who shall have the authority and responsi-  
 15          bility to—

16               “(A) lead the privacy program of the agency;  
 17          and

18               “(B) carry out the privacy responsibilities of  
 19          the agency under this chapter, section 552a of title  
 20          5, and guidance issued by the Director.

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

22               “(A) serve in a central leadership position with-  
 23          in the agency;

24               “(B) have visibility into relevant agency oper-  
 25          ations; and

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

4           “(3) A privacy officer of an agency established under  
5           a statute enacted before the date of enactment of the Fed-  
6           eral Information Security Modernization Act of 2023 may  
7           carry out the responsibilities under this subsection for the  
8           agency.”; and

9           (4) in section 3513—

10                   (A) by redesignating subsection (c) as sub-  
11                   section (d); and

12                   (B) by inserting after subsection (b) the  
13                   following:

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

18           (b) SUBCHAPTER H DEFINITIONS.—

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

21                           (A) by redesignating paragraphs (2), (3),  
22                           (4), (5), (6), and (7) as paragraphs (3), (4),  
23                           (5), (6), (8), and (10), respectively;

24                           (B) by inserting after paragraph (1) the  
25                   following:



1           ~~“(2) The term ‘high value asset’ means infor-~~  
 2           ~~mation or an information system that the head of an~~  
 3           ~~agency, using policies, principles, standards, or~~  
 4           ~~guidelines issued by the Director under section~~  
 5           ~~3553(a), determines to be so critical to the agency~~  
 6           ~~that the loss or degradation of the confidentiality,~~  
 7           ~~integrity, or availability of such information or infor-~~  
 8           ~~mation system would have a serious impact on the~~  
 9           ~~ability of the agency to perform the mission of the~~  
 10           ~~agency or conduct business.”;~~

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

13           ~~“(7) The term ‘major incident’ has the meaning~~  
 14           ~~given the term in guidance issued by the Director~~  
 15           ~~under section 3598(a).”;~~

16                   (D) in paragraph (8)(A), as so redesign-  
 17           ated, by striking “used” and inserting “owned,  
 18           managed,”;

19                   (E) by inserting after paragraph (8), as so  
 20           redesignated, the following:

21           ~~“(9) The term ‘penetration test’—~~

22                   ~~“(A) means an authorized assessment that~~  
 23           ~~emulates attempts to gain unauthorized access~~  
 24           ~~to, or disrupt the operations of, an information~~

system or component of an information system;  
and

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

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

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

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

(2) CONFORMING AMENDMENTS.—

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

(B) TITLE 10.—

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

by striking “section 3552(b)(6)(A)” and  
inserting “section 3552(b)(8)(A)”.

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

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

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

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

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

1        ~~provement Act of 2020 (15 U.S.C. 278g-3a(5))~~  
 2        is amended by striking “section 3552(b)(6)”  
 3        and inserting “section 3552(b)”.

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

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

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

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

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

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

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

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

(ii) in subsection (f)—

(I) in paragraph (3), by striking “section 3532(1)” and inserting “section 3552(b)”; and

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

(e) ~~SUBCHAPTER II AMENDMENTS.—~~Subchapter II of chapter 35 of title 44, United States Code, is amended—

(1) in section 3551—

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

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

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

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

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

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

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

21          ~~(2)~~ in section 3553—

22               (A) in subsection (a)—

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

1                   (ii) in paragraph (6), by striking the  
2                   period at the end and inserting “; and”;  
3                   and

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

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

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

15                  “(B) the use of presumption of com-  
16                  promise and least privilege principles, such as  
17                  zero trust architecture, to improve resiliency  
18                  and timely response actions to incidents on  
19                  Federal systems.”;

20                  (B) in subsection (b)—

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

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

chapter IV of this chapter” after “section 3556”;

(iii) by redesignating paragraphs (8) and (9) as paragraphs (10) and (11), respectively; and

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

“(8) expeditiously seeking opportunities to reduce costs, administrative burdens, and other barriers to information technology security and modernization for agencies, including through shared services for cybersecurity capabilities identified as appropriate by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and other agencies as appropriate;”;

(C) in subsection (c)—

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

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

(II) by inserting “, which shall be unclassified but may include 1 or more annexes that contain classified



1 or other sensitive information, as ap-  
 2 propriate” after “a report”; and

3 (III) by striking “preceding  
 4 year” and inserting “preceding 2  
 5 years”;

6 (ii) by striking paragraph (1);

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

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

12 (v) by inserting after paragraph (3),  
 13 as so redesignated, the following:

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

17 (D) in subsection (h)—

18 (i) in paragraph (2)—

19 (I) in subparagraph (A), by in-  
 20 serting “and the National Cyber Di-  
 21 rector” after “in coordination with the  
 22 Director”; and

23 (II) in subparagraph (D), by in-  
 24 serting “, the National Cyber Direc-  
 25 tor,” after “notify the Director”; and

1                   (ii) in paragraph (3)(A)(iv), by insert-  
 2                   ing “, the National Cyber Director,” after  
 3                   “the Secretary provides prior notice to the  
 4                   Director”;  
 5                   (E) by amending subsection (i) to read as  
 6                   follows:

7           “(i) ~~FEDERAL RISK ASSESSMENT.~~—On an ongoing  
 8 and continuous basis, the Director of the Cybersecurity  
 9 and Infrastructure Security Agency shall assess the Fed-  
 10 eral risk posture using any available information on the  
 11 cybersecurity posture of agencies, and brief the Director  
 12 and National Cyber Director on the findings of such as-  
 13 sessment, including—

14                   “(1) the status of agency cybersecurity remedial  
 15                   actions for high value assets described in section  
 16                   3554(b)(7);

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

20                   “(3) analysis of incident information under sec-  
 21                   tion 3597;

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

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

1           ~~“(6) evaluation of agency threat hunting re-~~  
2           ~~sults;~~

3           ~~“(7) evaluation of Federal and non-Federal~~  
4           ~~cyber threat intelligence;~~

5           ~~“(8) data on agency compliance with standards~~  
6           ~~issued under section 11331 of title 40;~~

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

9           ~~“(10) relevant reports from inspectors general~~  
10          ~~of agencies and the Government Accountability Of-~~  
11          ~~fice; and~~

12          ~~“(11) any other information the Director of the~~  
13          ~~Cybersecurity and Infrastructure Security Agency~~  
14          ~~determines relevant.”; and~~

15                 ~~(F) by adding at the end the following:~~

16          ~~“(m) DIRECTIVES.—~~

17                 ~~“(1) EMERGENCY DIRECTIVE UPDATES.—If the~~  
18          ~~Secretary issues an emergency directive under this~~  
19          ~~section, the Director of the Cybersecurity and Infra-~~  
20          ~~structure Security Agency shall submit to the Direc-~~  
21          ~~tor, the National Cyber Director, the Committee on~~  
22          ~~Homeland Security and Governmental Affairs of the~~  
23          ~~Senate, and the Committees on Oversight and Ae-~~  
24          ~~countability and Homeland Security of the House of~~  
25          ~~Representatives an update on the status of the im-~~

1        plementation of the emergency directive at agencies  
 2        not later than 7 days after the date on which the  
 3        emergency directive requires an agency to complete  
 4        a requirement specified by the emergency directive;  
 5        and every 30 days thereafter until—

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

8                “(B) the Secretary determines that an  
 9                emergency directive no longer requires active  
 10              reporting from agencies or additional implemen-  
 11              tation; or

12              “(C) the date that is 1 year after the  
 13              issuance of the directive.

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

ational directive, and every 90 days thereafter  
until—

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

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

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

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

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

1                   “(B) has not implemented a binding oper-  
2                   ational directive.

3           ~~“(n) REVIEW OF OFFICE OF MANAGEMENT AND~~  
4 ~~BUDGET GUIDANCE AND POLICY.—~~

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

12                  “(2) CONGRESSIONAL NOTIFICATION.—The Di-  
13                  rector of the Office of Management and Budget  
14                  shall notify the Committee on Homeland Security  
15                  and Governmental Affairs of the Senate and the  
16                  Committee on Oversight and Accountability of the  
17                  House of Representatives of changes to guidance or  
18                  policy resulting from the review under paragraph  
19                  (1).

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

24                  “(o) AUTOMATED STANDARD IMPLEMENTATION  
25 VERIFICATION.—When the Director of the National Insti-

1 tute of Standards and Technology issues a proposed  
 2 standard or guideline pursuant to paragraphs (2) or (3)  
 3 of section 20(a) of the National Institute of Standards and  
 4 Technology Act (15 U.S.C. 278g-3(a)), the Director of  
 5 the National Institute of Standards and Technology shall  
 6 consider developing and, if appropriate and practical, de-  
 7 velop specifications to enable the automated verification  
 8 of the implementation of the controls.

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

16               (3) in section 3554—

17                       (A) in subsection (a)—

18                               (i) in paragraph (1)—

19                                       (I) by redesignating subpara-  
 20 graphs (A), (B), and (C) as subpara-  
 21 graphs (B), (C), and (D), respectively;

22                                       (II) by inserting before subpara-  
 23 graph (B), as so redesignated, the fol-  
 24 lowing:

1           “(A) on an ongoing and continuous basis,  
2           assessing agency system risk, as applicable,  
3           by—

4                   “(i) identifying and documenting the  
5                   high value assets of the agency using guid-  
6                   ance from the Director;

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

11                  “(iii) identifying whether the agency  
12                  is participating in federally offered cyber-  
13                  security shared services programs;

14                  “(iv) identifying agency systems that  
15                  have access to or hold the data assets  
16                  inventoried under section 3511;

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

22                  “(vi) evaluating the vulnerability of  
23                  agency systems and data, including high  
24                  value assets, including by analyzing—



1 “(I) the results of penetration  
2 testing performed by the Department  
3 of Homeland Security under section  
4 3553(b)(9);

5 “(II) the results of penetration  
6 testing performed under section  
7 3559A;

8 “(III) information provided to  
9 the agency through the vulnerability  
10 disclosure program of the agency  
11 under section 3559B;

12 “(IV) incidents; and

13 “(V) any other vulnerability in-  
14 formation relating to agency systems  
15 that is known to the agency;

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

22 “(viii) assessing the consequences of  
23 potential incidents occurring on agency  
24 systems that would impact systems at  
25 other agencies, including due to

interconnectivity between different agency systems or operational reliance on the operations of the system or data in the system;”;

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking “providing information” and inserting “using information from the assessment required under subparagraph (A), providing information”;

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

(aa) in clause (ii) by inserting “binding” before “operational”; and

(bb) in clause (vi), by striking “and” at the end; and

(V) by adding at the end the following:

“(E) providing an update on the ongoing and continuous assessment required under subparagraph (A)—

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

“(ii) at intervals determined by guidance issued by the Director, and to the extent appropriate and practicable using automation, to—

“(I) the Director;

“(II) the Director of the Cybersecurity and Infrastructure Security Agency; and

“(III) the National Cyber Director;”;

(ii) in paragraph (2)—

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

(II) in subparagraph (D), by inserting “, through the use of penetration testing, the vulnerability disclosure program established under section 3559B, and other means,” after “periodically”;

1                   (iii) in paragraph (3)(A)—

2                   (I) in the matter preceding clause  
3                   (i), by striking “senior agency infor-  
4                   mation security officer” and inserting  
5                   “Chief Information Security Officer”;

6                   (II) in clause (i), by striking  
7                   “this section” and inserting “sub-  
8                   sections (a) through (e)”;

9                   (III) in clause (ii), by striking  
10                  “training and” and inserting “skills,  
11                  training, and”;

12                  (IV) by redesignating clauses (iii)  
13                  and (iv) as (iv) and (v), respectively;

14                  (V) by inserting after clause (ii)  
15                  the following:

16                  “(iii) manage information security, cy-  
17                  bersecurity budgets, and risk and compli-  
18                  ance activities and explain those concepts  
19                  to the head of the agency and the executive  
20                  team of the agency;”;

21                  (VI) in clause (iv), as so redesign-  
22                  ated, by striking “information secu-  
23                  rity duties as that official’s primary  
24                  duty” and inserting “information,  
25                  computer network, and technology se-

1 security duties as the Chief Information  
2 Security Officers' primary duty";

3 (iv) in paragraph (5), by striking "an-  
4 nually" and inserting "not less frequently  
5 than quarterly"; and

6 (v) in paragraph (6), by striking "offi-  
7 cial delegated" and inserting "Chief Infor-  
8 mation Security Officer delegated"; and  
9 (B) in subsection (b)—

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

12 "~~(1)~~ the ongoing and continuous assessment of  
13 agency system risk required under subsection  
14 (a)(1)(A), which may include using guidance and  
15 automated tools consistent with standards and  
16 guidelines promulgated under section ~~11331~~ of title  
17 40, as applicable";

18 (ii) in paragraph (2)—

19 (I) by striking subparagraph (B);

20 (II) by redesignating subpara-  
21 graphs (C) and (D) as subparagraphs  
22 (B) and (C), respectively;

23 (III) in subparagraph (B), as so  
24 redesignated, by striking "and" at the  
25 end; and

1                   (IV) in subparagraph (C), as so  
2 redesignated—

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

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

8                   “(iii) binding operational directives  
9 and emergency directives issued by the  
10 Secretary under section 3553;” and

11                   (cc) in clause (iv), as so re-  
12 designated, by striking “as deter-  
13 mined by the agency; and” and  
14 inserting “as determined by the  
15 agency, considering the agency  
16 risk assessment required under  
17 subsection (a)(1)(A);

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

21                   (iv) by redesignating paragraphs (7)  
22 and (8) as paragraphs (8) and (9), respec-  
23 tively;

24                   (v) by inserting after paragraph (6)  
25 the following:

1           “(7) a secure process for providing the status  
 2           of every remedial action and unremediated identified  
 3           system vulnerability of a high value asset to the Di-  
 4           rector and the Director of the Cybersecurity and In-  
 5           frastructure Security Agency, using automation and  
 6           machine-readable data to the greatest extent prac-  
 7           ticable;” and

8                         (vi) in paragraph (8)(C), as so redes-  
 9                         ignated—

10                        (I) by striking clause (ii) and in-  
 11                        serting the following:

12                        “(ii) notifying and consulting with the  
 13                        Federal information security incident cen-  
 14                        ter established under section 3556 pursu-  
 15                        ant to the requirements of section 3594;”;

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

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

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

23                        (IV) in clause (iv), as so redesign-  
 24                        ated—

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

3                               (bb) by striking subclause  
4                               (III); and

5                               (cc) by redesignating sub-  
6                               clause (IV) as subclause (III);  
7                               and

8                               (C) in subsection (c)—

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

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

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



1 security and Governmental Affairs of the Senate, the  
2 Committee on Oversight and Accountability of the  
3 House of Representatives, the Committee on Home-  
4 land Security of the House of Representatives, the  
5 Committee on Commerce, Science, and Transpor-  
6 tation of the Senate, the Committee on Science,  
7 Space, and Technology of the House of Representa-  
8 tives, and the appropriate authorization and appro-  
9 priations committees of Congress a report that—

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

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

22 “(C) summarizes the status of remedial ac-  
23 tions identified by inspector general of the  
24 agency, the Comptroller General of the United

1 States, and any other source determined appro-  
 2 priate by the head of the agency.

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

5 ~~“(A) shall be, to the greatest extent prae-~~  
 6 ~~ticable, in an unclassified and otherwise uncon-~~  
 7 ~~trolled form; and~~

8 ~~“(B) may include 1 or more annexes that~~  
 9 ~~contain classified or other sensitive information,~~  
 10 ~~as appropriate.~~

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

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

23 ~~(4) in section 3555—~~

(A) in the section heading, by striking  
~~“ANNUAL INDEPENDENT”~~ and inserting  
~~“INDEPENDENT”~~;

(B) in subsection (a)—

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

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

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

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

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

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

(E) in subsection (g)(2)—

1 (i) by striking “this subsection shall”  
 2 and inserting “this subsection—  
 3 “(A) shall”;

4 (ii) in subparagraph (A), as so des-  
 5 ignated, by striking the period at the end  
 6 and inserting “; and”; and

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

9 “(B) identify any entity that performs an  
 10 independent evaluation under subsection (b).”;  
 11 and

12 (F) by striking subsection (j) and inserting  
 13 the following:

14 “(j) GUIDANCE.—

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

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

1 “(A) the identification of the most common  
2 successful threat patterns;

3 “(B) the identification of security controls  
4 that address the threat patterns described in  
5 subparagraph (A);

6 “(C) any other security risks unique to  
7 Federal systems; and

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

10 ~~(5) in section 3556(a)—~~

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

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

17 ~~(d) CONFORMING AMENDMENTS.—~~

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

~~“3555. Independent evaluation.”.~~

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

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

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

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

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

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

(c) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

1           “SUBCHAPTER IV—FEDERAL SYSTEM  
2                           INCIDENT RESPONSE

3   **“§ 3591. Definitions**

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

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

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

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

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

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

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

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

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

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

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

3           “(I) the Director;

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

6           “(K) the National Cyber Director;

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

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

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

13               “(A) means—

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

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

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

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

22          “(3) Breach.—The term ‘breach’—

23               “(A) means the compromise, unauthorized  
24          disclosure, unauthorized acquisition, or loss of



1 control of personally identifiable information or  
2 any similar occurrence; and

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

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

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

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

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

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

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

9   **~~§ 3592. Notification of breach~~**

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

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

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

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

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

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

1 cy, in consultation with the Chief Information Officer and  
 2 Chief Privacy Officer of the agency, shall—

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

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

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

13              “(C) the type of breach; and

14              “(D) any other factors determined by the  
 15              Director; and

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

21              “(A) to the last known mailing address of  
 22              the individual; or

23              “(B) through an appropriate alternative  
 24              method of notification.

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

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

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

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

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

12              “(B) may include a telephone number,  
13       mailing address, or a website;

14              “(4) information on any remedy being offered  
15       by the agency;

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

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

1       “(d) ~~DELAY OF NOTIFICATION.—~~

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

9               “(A) ~~impede a criminal investigation or a~~  
10       national security activity;

11              “(B) ~~cause an adverse result (as described~~  
12       in section 2705(a)(2) of title 18);

13              “(C) ~~reveal sensitive sources and methods;~~

14              “(D) ~~cause damage to national security; or~~

15              “(E) ~~hamper security remediation actions.~~

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

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

23              “(e) ~~UPDATE NOTIFICATION.—~~If an agency deter-  
24       mines there is a significant change in the reasonable basis  
25       to conclude that a breach occurred, a significant change

1 to the determination made under subsection (b)(1), or that  
 2 it is necessary to update the details of the information pro-  
 3 vided to potentially affected individuals as described in  
 4 subsection (c); the agency shall as expeditiously as prac-  
 5 ticable and without unreasonable delay, and in any case  
 6 not later than 30 days after such a determination, notify  
 7 each individual who received a notification pursuant to  
 8 subsection (b) of those changes.

9 ~~“(f) DELAY OF NOTIFICATION REPORT.—~~

10 ~~“(1) IN GENERAL.—Not later than 1 year after~~  
 11 ~~the date of enactment of the Federal Information~~  
 12 ~~Security Modernization Act of 2023, and annually~~  
 13 ~~thereafter, the head of an agency, in coordination~~  
 14 ~~with any official who delays a notification under sub-~~  
 15 ~~section (d), shall submit to the appropriate reporting~~  
 16 ~~entities a report on each delay that occurred during~~  
 17 ~~the previous 2 years.~~

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

22 ~~“(g) CONGRESSIONAL REPORTING REQUIRE-~~  
 23 ~~MENTS.—~~

24 ~~“(1) REVIEW AND UPDATE.—On a periodic~~  
 25 ~~basis, the Director of the Office of Management and~~

1     Budget shall review, and update as appropriate,  
 2     breach notification policies and guidelines for agen-  
 3     cies.

4             ~~“(2) REQUIRED NOTICE FROM AGENCIES.—~~

5     Subject to paragraph (4), the Director of the Office  
 6     of Management and Budget shall require the head  
 7     of an agency affected by a covered breach to expedi-  
 8     tiously and not later than 30 days after the date on  
 9     which the agency discovers the covered breach give  
 10    notice of the breach, which may be provided elec-  
 11   tronically, to—

12            ~~“(A) each congressional committee de-~~  
 13            scribed in section 3554(c)(1); and

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

17            ~~“(3) CONTENTS OF NOTICE.—Notice of a cov-~~  
 18            ered breach provided by the head of an agency pur-  
 19            suant to paragraph (2) shall include, to the extent  
 20            practicable—

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

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

6           “(C) a description of any circumstances  
 7           necessitating a delay in providing notice to indi-  
 8           viduals affected by the covered breach in ac-  
 9           cordance 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  
 20           the House of Representatives;

21           “(C) the appropriations committees of  
 22           Congress;

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



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

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

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

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

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

13                 “(1) limit—

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

20                 “(B) the authority of the Director to issue  
21                 guidance relating to notifications and reporting  
22                 of breaches, covered breaches, or major inci-  
23                 dents;

24                 “(C) the authority of the head of an agen-  
25                 cy to provide more information than required

under subsection (b) when notifying individuals potentially affected by a breach;

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

~~“(i) the Director;~~

~~“(ii) the National Cyber Director;~~

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

~~“(iv) any other agency;~~

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

~~“(i) breaches that are not covered breaches; and~~

~~“(ii) additional information beyond the information described in subsection (g)(3); or~~

~~“(F) any Congressional reporting requirements of agencies under any other law; or~~

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

1 **“§ 3593. Congressional and Executive Branch reports**  
 2 **on major incidents**

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

6 ~~“(1) the majority and minority leaders of the~~  
 7 ~~Senate;~~

8 ~~“(2) the Speaker and minority leader of the~~  
 9 ~~House of Representatives;~~

10 ~~“(3) the Committee on Homeland Security and~~  
 11 ~~Governmental Affairs of the Senate;~~

12 ~~“(4) the Committee on Commerce, Science, and~~  
 13 ~~Transportation of the Senate;~~

14 ~~“(5) the Committee on Oversight and Account-~~  
 15 ~~ability of the House of Representatives;~~

16 ~~“(6) the Committee on Homeland Security of~~  
 17 ~~the House of Representatives;~~

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

20 ~~“(8) the appropriate authorization and appro-~~  
 21 ~~priations committees of Congress~~

22 ~~“(b) INITIAL NOTIFICATION.—~~

23 ~~“(1) IN GENERAL.—Not later than 72 hours~~  
 24 ~~after an agency has a reasonable basis to conclude~~  
 25 ~~that a major incident occurred, the head of the~~  
 26 ~~agency impacted by the major incident shall submit~~

1 to the appropriate reporting entities a written notifi-  
 2 cation, which may be submitted electronically and  
 3 include 1 or more annexes that contain classified or  
 4 other sensitive information, as appropriate.

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

10 “(A) A summary of the information avail-  
 11 able about the major incident, including how  
 12 the major incident occurred and the threat  
 13 causing the major incident.

14 “(B) If applicable, information relating to  
 15 any breach associated with the major incident,  
 16 regardless of whether—

17 “(i) the breach was the reason the in-  
 18 cident was determined to be a major inci-  
 19 dent; and

20 “(ii) head of the agency determined it  
 21 was appropriate to provide notification to  
 22 potentially impacted individuals pursuant  
 23 to section 3592(b)(1).

24 “(C) A preliminary assessment of the im-  
 25 pacts to—

1                   “(i) the agency;  
 2                   “(ii) the Federal Government;  
 3                   “(iii) the national security, foreign re-  
 4                   lations, homeland security, and economic  
 5                   security of the United States; and  
 6                   “(iv) the civil liberties, public con-  
 7                   fidence, privacy, and public health and  
 8                   safety of the people of the United States.

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

20               “(e) SUPPLEMENTAL UPDATE.—Within a reasonable  
 21               amount of time, but not later than 30 days after the date  
 22               on which the head of an agency submits a written notifica-  
 23               tion under subsection (a), the head of the agency shall  
 24               provide to the appropriate congressional entities an un-  
 25               classified and written update, which may include 1 or

1 more annexes that contain classified or other sensitive in-  
 2 formation, as appropriate, on the major incident, based  
 3 on information available to agency officials as of the date  
 4 on which the agency provides the update, on—

5 “(1) system vulnerabilities relating to the major  
 6 incident, where applicable, means by which the  
 7 major incident occurred, the threat causing the  
 8 major incident, where applicable, and impacts of the  
 9 major incident to—

10 “(A) the agency;

11 “(B) other Federal agencies, Congress, or  
 12 the judicial branch;

13 “(C) the national security, foreign rela-  
 14 tions, homeland security, or economic security  
 15 of the United States; or

16 “(D) the civil liberties, public confidence,  
 17 privacy, or public health and safety of the peo-  
 18 ple of the United States;

19 “(2) the status of compliance of the affected  
 20 Federal information system with applicable security  
 21 requirements at the time of the major incident;

22 “(3) if the major incident involved a breach, a  
 23 description of the affected information, an estimate  
 24 of the number of individuals potentially impacted,

1 and any assessment to the risk of harm to such indi-  
2 viduals;

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

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

11 “(d) ADDITIONAL UPDATE.—If the head of an agen-  
12 cy, the Director, or the National Cyber Director deter-  
13 mines that there is any significant change in the under-  
14 standing of the scope, scale, or consequence of a major  
15 incident for which the head of the agency submitted a  
16 written notification and update under subsections (b) and  
17 (c), the head of the agency shall submit to the appropriate  
18 congressional entities a written update that includes infor-  
19 mation relating to the change in understanding.

20 “(e) BIENNIAL REPORT.—Each agency shall submit  
21 as part of the biennial report required under section  
22 3554(c)(1) a description of each major incident that oc-  
23 curred during the 2-year period preceding the date on  
24 which the biennial report is submitted.

25 “(f) REPORT DELIVERY.—

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

3           ~~“(A) shall be submitted in an electronic~~  
 4           ~~format; and~~

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

6           ~~“(2) CLASSIFICATION STATUS.—Any written~~  
 7           ~~notification or update required to be submitted~~  
 8           ~~under this section—~~

9           ~~“(A) shall be—~~

10           ~~“(i) unclassified; and~~

11           ~~“(ii) submitted through unclassified~~  
 12           ~~electronic means pursuant to paragraph~~  
 13           ~~(1)(A); and~~

14           ~~“(B) may include classified annexes, as ap-~~  
 15           ~~propriate.~~

16           ~~“(g) REPORT CONSISTENCY.—To achieve consistent~~  
 17           ~~and coherent agency reporting to Congress, the National~~  
 18           ~~Cyber Director, in coordination with the Director, shall—~~

19           ~~“(1) provide recommendations to agencies on~~  
 20           ~~formatting and the contents of information to be in-~~  
 21           ~~cluded in the reports required under this section, in-~~  
 22           ~~cluding recommendations for consistent formats for~~  
 23           ~~presenting any associated metrics; and~~



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

4                   “(A) include, at a minimum—

5                           “(i) the full contents of the written  
6                           notification or update;

7                           “(ii) the identity of the reporting  
8                           agency; and

9                           “(iii) the date of submission; and

10                          “(iv) a list of the recipient congres-  
11                          sional entities; and

12                          “(B) be made available upon request to the  
13                          majority and minority leaders of the Senate, the  
14                          Speaker and minority leader of the House of  
15                          Representatives, the Committee on Homeland  
16                          Security and Governmental Affairs of the Sen-  
17                          ate, and the Committee on Oversight and Ae-  
18                          countability of the House of Representatives.

19           “(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL  
20           REPORTING EXEMPTION.—With respect to a major inci-  
21           dent that occurs exclusively on a national security system,  
22           the head of the affected agency shall submit the notifica-  
23           tions and reports required to be submitted to Congress  
24           under this section only to—

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 appropriations committees of Con-~~  
 6     ~~gress;~~

7           ~~“(4) the appropriate authorization committees~~  
 8     ~~of Congress;~~

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

11          ~~“(6) the Select Committee on Intelligence of the~~  
 12    ~~Senate;~~

13          ~~“(7) the Committee on Oversight and Account-~~  
 14    ~~ability of the House of Representatives; and~~

15          ~~“(8) the Permanent Select Committee on Intel-~~  
 16    ~~ligence of the House of Representatives.~~

17    ~~“(i) MAJOR INCIDENTS INCLUDING BREACHES.—If~~  
 18    ~~a major incident constitutes a covered breach, as defined~~  
 19    ~~in section 3592(a), information on the covered breach re-~~  
 20    ~~quired to be submitted to Congress pursuant to section~~  
 21    ~~3592(g) may—~~

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

24          ~~“(2) be reported to Congress under the process~~  
 25    ~~established under section 3592(g).~~

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

3               “(1) limit—

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

6                       “(B) Congress from requesting additional  
7 information from agencies through reports,  
8 briefings, or other means;

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

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

13       **“§ 3594. Government information sharing and inci-**  
14               **dent response**

15               “(a) **IN GENERAL.**—

16                       “(1) **INCIDENT SHARING.**—Subject to para-  
17 graph (4) and subsection (b), and in accordance  
18 with the applicable requirements pursuant to section  
19 3553(b)(2)(A) for reporting to the Federal informa-  
20 tion security incident center established under sec-  
21 tion 3556, the head of each agency shall provide to  
22 the Cybersecurity and Infrastructure Security Agen-  
23 cy information relating to any incident affecting the  
24 agency, whether the information is obtained by the  
25 Federal Government directly or indirectly.

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

5           “(A) a full description of the incident, in-  
6 cluding—

7           “(i) all indicators of compromise and  
8 tactics, techniques, and procedures;

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

13           “(iii) information that would support  
14 enabling defensive measures; and

15           “(iv) other information that may as-  
16 sist in identifying other victims;

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

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

23           “(i) a description of the affected sys-  
24 tems or networks;

1           “(ii) the estimated dates of when the  
2           incident occurred; and

3           “(iii) information that could reason-  
4           ably help identify any malicious actor that  
5           may have conducted or caused the inci-  
6           dent, subject to appropriate privacy protec-  
7           tions.

8           “(3) INFORMATION SHARING.—The Director of  
9           the Cybersecurity and Infrastructure Security Agen-  
10          cy shall—

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

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

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

18                   “(I) impacted by the incident;

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

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

23           “(ii) appropriate Federal law enforce-  
24           ment agencies to facilitate any necessary  
25           threat response activities, as requested;

1           ~~“(C) coordinate any necessary information~~  
2           ~~sharing efforts relating to a major incident with~~  
3           ~~the private sector; and~~

4           ~~“(D) notify the National Cyber Director of~~  
5           ~~any efforts described in subparagraph (C).~~

6           ~~“(4) NATIONAL SECURITY SYSTEMS EXEMP-~~  
7           ~~TION.—~~

8           ~~“(A) IN GENERAL.—Notwithstanding~~  
9           ~~paragraphs (1) and (3), each agency operating~~  
10          ~~or exercising control of a national security sys-~~  
11          ~~tem shall share information about an incident~~  
12          ~~that occurs exclusively on a national security~~  
13          ~~system with the Secretary of Defense, the Di-~~  
14          ~~rector, the National Cyber Director, and the~~  
15          ~~Director of the Cybersecurity and Infrastruc-~~  
16          ~~ture Security Agency to the extent consistent~~  
17          ~~with standards and guidelines for national secu-~~  
18          ~~rity systems issued in accordance with law and~~  
19          ~~as directed by the President.~~

20          ~~“(B) PROTECTIONS.—Any information~~  
21          ~~sharing and handling of information under this~~  
22          ~~paragraph shall be appropriately protected con-~~  
23          ~~sistent with procedures authorized for the pro-~~  
24          ~~tection of sensitive sources and methods or by~~  
25          ~~procedures established for information that~~

1           have been specifically authorized under criteria  
 2           established by an Executive order or an Act of  
 3           Congress to be kept classified in the interest of  
 4           national defense or foreign policy.

5       “(b) AUTOMATION.—In providing information and  
 6 selecting a method to provide information under sub-  
 7 section (a), the head of each agency shall implement sub-  
 8 section (a)(1) in a manner that provides such information  
 9 to the Cybersecurity and Infrastructure Security Agency  
 10 in an automated and machine-readable format, to the  
 11 greatest extent practicable.

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

17           “(1) the Cybersecurity and Infrastructure Secu-  
 18 rity Agency to facilitate asset response activities and  
 19 provide recommendations for mitigating future inci-  
 20 dents; and

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

24   **“§ 3595. Responsibilities of contractors and awardees**

25       “(a) REPORTING.—

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

5           “(A) an incident or breach has occurred  
6 with respect to Federal information the con-  
7 tractor or awardee collected, used, or main-  
8 tained on behalf of an agency;

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

13           “(C) a component of any Federal informa-  
14 tion system operated, managed, or maintained  
15 by a contractor or awardee contains a security  
16 vulnerability, including a supply chain com-  
17 promise or an identified software or hardware  
18 vulnerability, for which there is reliable evidence  
19 of attempted or successful exploitation of the  
20 vulnerability by an actor without authorization  
21 of the Federal information system owner; or

22           “(D) the contractor or awardee has re-  
23 ceived personally identifiable information, per-  
24 sonal health information, or other clearly sen-  
25 sitive information that is beyond the scope of



1 the contract or agreement with the agency from  
2 the agency that the contractor or awardee is  
3 not authorized to receive.

4 “(2) THIRD-PARTY REPORTS OF  
5 VULNERABILITIES.—Subject to the guidance issued  
6 by the Director pursuant to paragraph (4), any con-  
7 tractor or awardee of an agency shall report to the  
8 agency and the Cybersecurity and Infrastructure Se-  
9 curity Agency if the contractor or awardee has a  
10 reasonable basis to suspect or conclude that a com-  
11 ponent of any Federal information system operated,  
12 managed, or maintained on behalf of an agency by  
13 the contractor or awardee on behalf of the agency  
14 contains a security vulnerability, including a supply  
15 chain compromise or an identified software or hard-  
16 ware vulnerability, that has been reported to the  
17 contractor or awardee by a third party, including  
18 through a vulnerability disclosure program.

19 “(3) PROCEDURES.—

20 “(A) SHARING WITH CISA.—As soon as  
21 practicable following a report of an incident to  
22 an agency by a contractor or awardee under  
23 paragraph (1), the head of the agency shall pro-  
24 vide, pursuant to section 3594, information

1 about the incident to the Director of the Cyber-  
2 security and Infrastructure Security Agency.

3 “(B) TIME FOR REPORTING.—Unless a  
4 different time for reporting is specified in a  
5 contract, grant, cooperative agreement, or other  
6 transaction agreement, a contractor or awardee  
7 shall—

8 “(i) make a report required under  
9 paragraph (1) not later than 1 day after  
10 the date on which the contractor or award-  
11 ee has reasonable basis to suspect or con-  
12 clude that the criteria under paragraph (1)  
13 have been met; and

14 “(ii) make a report required under  
15 paragraph (2) within a reasonable time;  
16 but not later than 90 days after the date  
17 on which the contractor or awardee has  
18 reasonable basis to suspect or conclude  
19 that the criteria under paragraph (2) have  
20 been met.

21 “(C) PROCEDURES.—Following a report of  
22 a breach or incident to an agency by a con-  
23 tractor or awardee under paragraph (1), the  
24 head of the agency, in consultation with the  
25 contractor or awardee, shall carry out the appli-

1 cable requirements under sections ~~3592~~, ~~3593~~,  
 2 and ~~3594~~ with respect to the breach or inci-  
 3 dent.

4 “(D) RULE OF CONSTRUCTION.—Nothing  
 5 in subparagraph (B) shall be construed to allow  
 6 the negation of the requirements to report  
 7 vulnerabilities under paragraph (1) or (2)  
 8 through a contract, grant, cooperative agree-  
 9 ment, or other transaction agreement.

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

16 “(b) REGULATIONS; MODIFICATIONS.—

17 “(1) IN GENERAL.—Not later than 1 year after  
 18 the date of enactment of the Federal Information  
 19 Security Modernization Act of 2023—

20 “(A) the Federal Acquisition Regulatory  
 21 Council shall promulgate regulations, as appro-  
 22 priate, relating to the responsibilities of con-  
 23 tractors and recipients of other transaction  
 24 agreements and cooperative agreements to com-  
 25 ply with this section; and

1           “(B) the Office of Federal Financial Man-  
 2           agement shall promulgate regulations under  
 3           title 2, Code Federal Regulations, as appro-  
 4           priate, relating to the responsibilities of grant-  
 5           ees to comply with this section.

6           “(2) IMPLEMENTATION.—Not later than 1 year  
 7           after the date on which the Federal Acquisition Reg-  
 8           ulatory Council and the Office of Federal Financial  
 9           Management promulgates regulations under para-  
 10          graph (1), the head of each agency shall implement  
 11          policies and procedures, as appropriate, necessary to  
 12          implement those regulations.

13          “(3) CONGRESSIONAL NOTIFICATION.—

14           “(A) IN GENERAL.—The head of each  
 15           agency head shall notify the Director upon im-  
 16           plementation of policies and procedures nec-  
 17           essary to implement the regulations promul-  
 18           gated under paragraph (1).

19           “(B) OMB NOTIFICATION.— Not later  
 20           than 30 days after the date described in para-  
 21           graph (2), the Director shall notify the Com-  
 22           mittee on Homeland Security and Govern-  
 23           mental Affairs of the Senate and the Commit-  
 24           tees on Oversight and Accountability and  
 25           Homeland Security of the House of Representa-

1           tives on the status of the implementation by  
 2           each agency of the regulations promulgated  
 3           under paragraph (1).

4           “(c) NATIONAL SECURITY SYSTEMS EXEMPTION.—

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

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

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

15   **“§ 3596. Training**

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

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

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

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

1 Agency, in consultation with the Director, the National  
 2 Cyber Director, and the Director of the National Institute  
 3 of Standards and Technology, shall develop best practices  
 4 to support consistency across agencies in cybersecurity in-  
 5 cident response training, including—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

13          “(e) PUBLICATION.—

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

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

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

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

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

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

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

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

22 ~~“(ii) in consultation with the impacted~~  
 23 ~~agency; and~~

24 ~~“(iii) in consultation with the inspec-~~  
 25 ~~tor general of the impacted agency.~~

1       “(d) INFORMATION PROVIDED BY AGENCIES.—

2               “(1) IN GENERAL.—The analysis required  
3       under subsection (a) and each report submitted  
4       under subsection (b) shall use information provided  
5       by agencies under section 3594(a).

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

16      “(e) NATIONAL SECURITY SYSTEM REPORTS.—

17              “(1) IN GENERAL.—Notwithstanding any other  
18      provision of this section, the Secretary of Defense, in  
19      consultation with the Director, the National Cyber  
20      Director, the Director of National Intelligence, and  
21      the Director of Cybersecurity and Infrastructure Se-  
22      curity shall annually submit a report that includes  
23      the information described in subsection (b) with re-  
24      spect to national security systems, to the extent that  
25      the submission is consistent with standards and

1 guidelines for national security systems issued in ac-  
2 cordance with law and as directed by the President,  
3 to—

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

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

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

10 “(D) the Select Committee on Intelligence  
11 of the Senate;

12 “(E) the Committee on Armed Services of  
13 the Senate;

14 “(F) the Committee on Appropriations of  
15 the Senate;

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

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

20 “(I) the Permanent Select Committee on  
21 Intelligence of the House of Representatives;

22 “(J) the Committee on Armed Services of  
23 the House of Representatives; and

24 “(K) the Committee on Appropriations of  
25 the House of Representatives.

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

4   **“§ 3598. Major incident definition**

5           “(a) ~~IN GENERAL.~~—Not later than 1 year after the  
 6           later of the date of enactment of the Federal Information  
 7           Security Modernization Act of 2023 and the most recent  
 8           publication by the Director of guidance to agencies regard-  
 9           ing major incidents as of the date of enactment of the  
 10          Federal Information Security Modernization Act of 2023,  
 11          the Director shall develop, in coordination with the Na-  
 12          tional Cyber Director, and promulgate guidance on the  
 13          definition of the term ‘major incident’ for the purposes  
 14          of subchapter II and this subchapter.

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

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

21                         “(A) any incident the head of the agency  
 22                         determines is likely to result in demonstrable  
 23                         harm to—

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

4           “(ii) the civil liberties, public con-  
5           fidence, privacy, or public health and safe-  
6           ty of the people of the United States;

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

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

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

22          “(E) any other type of incident determined  
23          appropriate by the Director;

24          “(2) stipulate that the National Cyber Director,  
25          in consultation with the Director and the Director of

1 the Cybersecurity and Infrastructure Security Agen-  
 2 cy, may declare a major incident at any agency, and  
 3 such a declaration shall be considered if it is deter-  
 4 mined that an incident—

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

7 “(B) is enabled by—

8 “(i) a common technical root cause,  
 9 such as a supply chain compromise, or a  
 10 common software or hardware vulner-  
 11 ability; or

12 “(ii) the related activities of a com-  
 13 mon threat actor;

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

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

23 “(c) EVALUATION AND UPDATES.—Not later than 60  
 24 days after the date on which the Director first promul-  
 25 gates the guidance required under subsection (a), and not



1 less frequently than once during the first 90 days of each  
 2 evenly numbered Congress thereafter, the Director shall  
 3 provide to the Committee on Homeland Security and Gov-  
 4 ernmental Affairs of the Senate and the Committees on  
 5 Oversight and Accountability and Homeland Security of  
 6 the House of Representatives a briefing that includes—

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

9           “(2) an evaluation of any necessary updates to  
 10       the definition of the term ‘major incident’ included  
 11       in the guidance; and

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

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

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions:

“3592. Notification of breach:

“3593. Congressional and Executive Branch reports:

“3594. Government information sharing and incident response:

“3595. Responsibilities of contractors and awardees:

“3596. Training:

“3597. Analysis and report on Federal incidents:

“3598. Major incident definition.”.

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

18       (a) MODERNIZING GOVERNMENT TECHNOLOGY.—

19 Subtitle G of title X of division A of the National Defense  
 20 Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301  
 21 note) is amended in section 1078—

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

3           “(a) DEFINITIONS.—In this section:

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

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

10          (2) in subsection (b), by adding at the end the  
11 following:

12          “(8) PROPOSAL EVALUATION.—The Director  
13 shall—

14               “(A) give consideration for the use of  
15 amounts in the Fund to improve the security of  
16 high value assets; and

17               “(B) require that any proposal for the use  
18 of amounts in the Fund includes, as appro-  
19 priate—

20                       “(i) a cybersecurity risk management  
21 plan; and

22                       “(ii) a supply chain risk assessment in  
23 accordance with section 1326 of title 41.”;  
24 and

25          (3) in subsection (c)—

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

(B) in paragraph (5)—

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

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

(iii) by adding at the end the following:

“(C) a senior official from the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, appointed by the Director.”; and

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

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

(1) in section 11302—

(A) in subsection (b), by striking “use, security, and disposal of” and inserting “use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Se-

1 security Agency and the National Cyber Director,  
2 promote and improve the security of,”; and

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

6 (2) in section 11303(b)(2)(B)—

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

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

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

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

15 (c) SUBCHAPTER H.—Subchapter H of chapter 113  
16 of subtitle III of title 40, United States Code, is amend-  
17 ed—

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

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

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

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

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

6           (a) RESPONSIBILITIES OF THE CYBERSECURITY AND  
 7   INFRASTRUCTURE SECURITY AGENCY.—

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

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

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

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

1           ~~(B)~~ provide to the appropriate congressional  
2           committees a briefing on the plan developed  
3           under subparagraph ~~(A)~~.

4           ~~(2) BRIEFING.~~—Not later than 1 year after the  
5           date of enactment of this Act, the Director of the  
6           Cybersecurity and Infrastructure Security Agency  
7           shall provide to the appropriate congressional committees  
8           a briefing on—

9                   ~~(A)~~ the execution of the plan required  
10           under paragraph ~~(1)(A)~~; and

11                   ~~(B)~~ the development of the report required  
12           under section ~~3597(b)~~ of title 44, United States  
13           Code, as added by this Act.

14           ~~(b) RESPONSIBILITIES OF THE DIRECTOR OF THE~~  
15           ~~OFFICE OF MANAGEMENT AND BUDGET.~~—

16           ~~(1) UPDATING FISMA 2014.~~—Section 2 of the  
17           Federal Information Security Modernization Act of  
18           2014 (~~Public Law 113–283~~, ~~128 Stat. 3073~~) is  
19           amended—

20                   ~~(A)~~ by striking subsections ~~(b)~~ and ~~(d)~~;  
21           and

22                   ~~(B)~~ by redesignating subsections ~~(c)~~, ~~(e)~~,  
23           and ~~(f)~~ as subsections ~~(b)~~, ~~(e)~~, and ~~(d)~~, respectively.  
24           

25           ~~(2) INCIDENT DATA SHARING.~~—

1           (A) ~~IN GENERAL.~~—The Director, in coordi-  
 2 nation with the Director of the Cybersecurity  
 3 and Infrastructure Security Agency, shall de-  
 4 velop, and as appropriate update, guidance, on  
 5 the content, timeliness, and format of the infor-  
 6 mation provided by agencies under section  
 7 3594(a) of title 44, United States Code, as  
 8 added by this Act.

9           (B) ~~REQUIREMENTS.~~—The guidance devel-  
 10 oped under subparagraph (A) shall—

11                 (i) enable the efficient development  
 12 of—

13                         (I) lessons learned and rec-  
 14 ommendations in responding to, recov-  
 15 ering from, remediating, and miti-  
 16 gating future incidents; and

17                         (II) the report on Federal inci-  
 18 dents required under section 3597(b)  
 19 of title 44, United States Code, as  
 20 added by this Act; and

21                 (ii) include requirements for the time-  
 22 liness of data production.

23           (C) ~~AUTOMATION.~~—The Director, in co-  
 24 ordination with the Director of the Cybersecu-  
 25 rity and Infrastructure Security Agency, shall

promote, as feasible, the use of automation and machine-readable data for data sharing under section 3594(a) of title 44, United States Code, as added by this Act.

~~(3) CONTRACTOR AND Awardee GUIDANCE.—~~

~~(A) IN GENERAL.—~~Not later than 1 year after the date of enactment of this Act, the Director shall issue guidance to agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this Act.

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

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

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



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

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

4           “(13) to another agency, to the extent nec-  
5           essary, to assist the recipient agency in responding  
6           to an incident (as defined in section 3552 of title  
7           44) or breach (as defined in section 3591 of title 44)  
8           or to fulfill the information sharing requirements  
9           under section 3594 of title 44.”.

10 **SEC. 6. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**  
11 **UPDATES.**

12       (a) **IN GENERAL.**—Not later than 1 year after the  
13 date of enactment of this Act, the Director shall issue  
14 guidance for agencies on—

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

19           (2) establishing a process for securely providing  
20 the status of each remedial action for high value as-  
21 sets under section 3554(b)(7) of title 44, United  
22 States Code, as amended by this Act, to the Director  
23 and the Director of the Cybersecurity and Infra-  
24 structure Security Agency using automation and ma-

1 machine-readable data, as practicable, which shall in-  
 2 clude—

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

5 (B) templates for providing the status of  
 6 the remedial action.

7 (b) COORDINATION.—The head of each agency shall  
 8 coordinate with the inspector general of the agency, as ap-  
 9 plicable, to ensure consistent understanding of agency  
 10 policies for the purpose of evaluations conducted by the  
 11 inspector general.

12 **SEC. 7. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SEC-**  
 13 **TOR ENTITIES IMPACTED BY INCIDENTS.**

14 (a) DEFINITIONS.—In this section:

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

19 (2) SENSITIVE INFORMATION.—The term “sen-  
 20 sitive information” has the meaning given the term  
 21 by the Director in guidance issued under subsection

22 (b).

23 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-  
 24 TITIES.—Not later than 1 year after the date of enact-  
 25 ment of this Act, the Director shall develop, in consulta-

tion with the National Cyber Director, and issue guidance requiring the head of each agency to notify a reporting entity, and take into consideration the need to coordinate with Sector Risk Management Agencies (as defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)), as appropriate, of an incident at the agency that is likely to substantially affect—

(1) the confidentiality or integrity of sensitive information submitted by the reporting entity to the agency pursuant to a statutory or regulatory requirement; or

(2) any information system (as defined in section 3502 of title 44, United States Code) used in the transmission or storage of the sensitive information described in paragraph (1).

#### **SEC. 8. MOBILE SECURITY BRIEFINGS.**

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

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

(2) as a component of the briefing required under paragraph (1), a list of each exception of an agency from the No TikTok on Government Devices

1 Act (44 U.S.C. 3553 note; Public Law 117-328),  
 2 which may include a classified annex.

3 (b) ~~ADDITIONAL BRIEFING.~~—Not later than 1 year  
 4 after the date of the briefing required under subsection  
 5 (a)(1), the Director shall provide to the appropriate con-  
 6 gressional committees—

7 (1) a briefing on the compliance of any agency  
 8 that was not compliant with the No TikTok on Gov-  
 9 ernment Devices Act (44 U.S.C. 3553 note; Public  
 10 Law 117-328) at the time of the briefing required  
 11 under subsection (a)(1); and

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

15 **SEC. 9. DATA AND LOGGING RETENTION FOR INCIDENT RE-**  
 16 **SPONSE.**

17 (a) ~~GUIDANCE.~~—Not later than 2 years after the date  
 18 of enactment of this Act the Director, in consultation with  
 19 the National Cyber Director and the Director of the Cy-  
 20 bersecurity and Infrastructure Security Agency, shall up-  
 21 date guidance to agencies regarding requirements for log-  
 22 ging, log retention, log management, sharing of log data  
 23 with other appropriate agencies, or any other logging ac-  
 24 tivity determined to be appropriate by the Director.

1       (b) NATIONAL SECURITY SYSTEMS.—The Secretary  
 2 of Defense shall issue guidance that meets or exceeds the  
 3 standards required in guidance issued under subsection  
 4 (a) for National Security Systems.

5 **SEC. 10. CISA AGENCY LIAISONS.**

6       (a) IN GENERAL.—Not later than 120 days after the  
 7 date of enactment of this Act, the Director of the Cyberse-  
 8 curity and Infrastructure Security Agency shall assign not  
 9 less than 1 cybersecurity professional employed by the Cy-  
 10 bersecurity and Infrastructure Security Agency to be the  
 11 Cybersecurity and Infrastructure Security Agency liaison  
 12 to the Chief Information Security Officer of each agency.

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

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

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

- 21               (1) providing, as requested, assistance and ad-
- 22               vice to the agency Chief Information Security Offi-
- 23               cer;

1           (2) supporting, as requested, incident response  
 2           coordination between the assigned agency and the  
 3           Cybersecurity and Infrastructure Security Agency;

4           (3) becoming familiar with assigned agency sys-  
 5           tems, processes, and procedures to better facilitate  
 6           support to the agency; and

7           (4) other liaison duties to the assigned agency  
 8           solely in furtherance of Federal cybersecurity or sup-  
 9           port to the assigned agency as a Sector Risk Man-  
 10          agement Agency, as assigned by the Director of the  
 11          Cybersecurity and Infrastructure Security Agency in  
 12          consultation with the head of the assigned agency.

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

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

18          (f) COORDINATION OF ACTIVITIES.—The Director of  
 19          the Cybersecurity and Infrastructure Security Agency  
 20          shall consult with the Director on the execution of the du-  
 21          ties of the Cybersecurity and Infrastructure Security  
 22          Agency liaisons to ensure that there is no inappropriate  
 23          duplication of activities among—

24                (1) Federal cybersecurity support to agencies of  
 25                the Office of Management and Budget; and

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

3           (g) **RULE OF CONSTRUCTION.**—Nothing in this see-  
4           tion shall be construed impact the ability of the Director  
5           to support agency implementation of Federal cybersecurity  
6           requirements pursuant to subchapter II of chapter 35 of  
7           title 44, United States Code, as amended by this Act.

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

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

12         **“§ 3559A. Federal penetration testing**

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

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

19                         “(2) provides policies governing the develop-  
20                         ment of—

21                                 “(A) rules of engagement for using pene-  
22                                 tration testing; and

23                                 “(B) procedures to use the results of pene-  
24                                 tration testing to improve the cybersecurity and  
25                                 risk management of the agency;

1           ~~“(3) ensures that operational support or a~~  
 2           ~~shared service is available; and~~

3           ~~“(4) in no manner restricts the authority of the~~  
 4           ~~Secretary of Homeland Security or the Director of~~  
 5           ~~the Cybersecurity and Infrastructure Agency to con-~~  
 6           ~~duct threat hunting pursuant to section 3553 of title~~  
 7           ~~44, United States Code, or penetration testing under~~  
 8           ~~this chapter.~~

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

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

15                 ~~“(1) the Secretary of Defense in the case of a~~  
 16                 ~~system described in section 3553(e)(2); and~~

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

19          ~~(b) EXISTING GUIDANCE.—~~

20                 ~~(1) IN GENERAL.—Compliance with guidance~~  
 21                 ~~issued by the Director relating to penetration testing~~  
 22                 ~~before the date of enactment of this Act shall be~~  
 23                 ~~deemed to be compliance with section 3559A of title~~  
 24                 ~~44, United States Code, as added by this Act.~~



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

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

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

“3559A. Federal penetration testing.”.

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

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

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

1                   “(B) with prior notification to the head of  
2                   the agency;”.

3 **SEC. 12. VULNERABILITY DISCLOSURE POLICIES.**

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

7 **“§ 3559B. Federal vulnerability disclosure policies**

8       “(a) **PURPOSE; SENSE OF CONGRESS.**—

9               “(1) **PURPOSE.**—The purpose of Federal vul-  
10 nerability disclosure policies is to create a mecha-  
11 nism to enable the public to inform agencies of  
12 vulnerabilities in Federal information systems.

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

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

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

22              “(2) **INTERNET OF THINGS.**—The term ‘inter-  
23 net of things’ has the meaning given the term in  
24 Special Publication 800–213 of the National Insti-  
25 tute of Standards and Technology, entitled ‘IoT De-

1 vice Cybersecurity Guidance for the Federal Govern-  
 2 ment: Establishing IoT Device Cybersecurity Re-  
 3 quirements<sup>2</sup>, or any successor document.

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

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

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

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

18 “(1) use of the information system security  
 19 vulnerabilities disclosure process guidelines estab-  
 20 lished under section 4(a)(1) of the IoT Cybersecurity  
 21 Improvement Act of 2020 (15 U.S.C. 278g–  
 22 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 ef-  
5           fort to follow the vulnerability disclosure policy  
6           of the 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  
19          by a submitter of a security vulnerability, without a  
20          significant compromise of confidentiality, integrity,  
21          or availability, does not constitute a major incident;  
22          and

23          “(7) the applicability of the guidance to Inter-  
24          net of things devices owned or controlled by an  
25          agency.

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

5       “(e) RESPONSIBILITIES OF CISA.—The Director of  
 6       the Cybersecurity and Infrastructure Security Agency  
 7       shall—

8               “(1) provide support to agencies with respect to  
 9       the implementation of the requirements of this sec-  
 10      tion;

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

15              “(3) upon a request by an agency, assist the  
 16      agency in the disclosure to vendors of newly identi-  
 17      fied security vulnerabilities in vendor products and  
 18      services; and

19              “(4) as appropriate, implement the require-  
 20      ments of this section, in accordance with the author-  
 21      ity under section 3553(b)(8), as a shared service  
 22      available to agencies.

23       “(f) RESPONSIBILITIES OF AGENCIES.—

24              “(1) PUBLIC INFORMATION.—The head of each  
 25      agency shall make publicly available, with respect to

1 each internet domain under the control of the agen-  
 2 cy that is not a national security system and to the  
 3 extent consistent with the security of information  
 4 systems but with the presumption of disclosure—

5 “(A) an appropriate security contact; and

6 “(B) the component of the agency that is  
 7 responsible for the internet accessible services  
 8 offered at the domain.

9 “(2) VULNERABILITY DISCLOSURE POLICY.—

10 The head of each agency shall develop and make  
 11 publicly available a vulnerability disclosure policy for  
 12 the agency, which shall—

13 “(A) describe—

14 “(i) the scope of the systems of the  
 15 agency included in the vulnerability disclo-  
 16 sure policy, including for Internet of things  
 17 devices owned or controlled by the agency;

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

20 “(iii) the type of information system  
 21 testing that is not authorized by the agen-  
 22 cy;

23 “(iv) the disclosure policy for a con-  
 24 tractor; and

1                   “(v) the disclosure policy of the agen-  
2                   cy for sensitive information;

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

5                   “(i) how the submitter should submit  
6                   the vulnerability disclosure report; and

7                   “(ii) if the report is not anonymous,  
8                   when the reporter should anticipate an ac-  
9                   knowledge of receipt of the report by  
10                  the agency;

11                  “(C) include any other relevant informa-  
12                  tion; and

13                  “(D) be mature in scope and cover every  
14                  internet accessible information system used or  
15                  operated by that agency or on behalf of that  
16                  agency.

17                  “(3)               IDENTIFIED               SECURITY  
18                  VULNERABILITIES.—The head of each agency  
19                  shall—

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

22                  “(B) commensurate with the risk posed by  
23                  the security vulnerability, address such security  
24                  vulnerability using the security vulnerability  
25                  management process of the agency; and

1           “(C) in accordance with subsection (c)(5);  
 2           provide information to the submitter of a vul-  
 3           nerability disclosure report.

4           “(g) EXEMPTIONS.—

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

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

17               “(A) disrupt a law enforcement investiga-  
 18               tion;

19               “(B) endanger national security or intel-  
 20               ligence activities; or

21               “(C) impede national defense activities or  
 22               military operations.

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



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

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

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

9       “(i) REVISION OF FEDERAL ACQUISITION REGULA-  
10 TION.—The Federal Acquisition Regulation shall be re-  
11 vised as necessary to implement the provisions under this  
12 section.”.

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

“3559B. Federal vulnerability disclosure policies.”.

17       (c) CONFORMING UPDATE AND REPEAL.—

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

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

4                   (A) by striking section 6 (15 U.S.C. 278g–  
 5                   3d); and

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

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

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

16                   (1) shifting away from trusted networks to im-  
 17                   plement security controls based on a presumption of  
 18                   compromise, including through the transition to zero  
 19                   trust architecture;

20                   (2) implementing principles of least privilege in  
 21                   administering information security programs;

22                   (3) limiting the ability of entities that cause in-  
 23                   cidents to move laterally through or between agency  
 24                   systems;

25                   (4) identifying incidents quickly;

1           (5) isolating and removing unauthorized entities  
 2           from agency systems as quickly as practicable; ac-  
 3           counting for intelligence or law enforcement pur-  
 4           poses; and

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

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

15                (1) a description of steps agencies have com-  
 16                pleted, including progress toward achieving any re-  
 17                quirements issued by the Director, including the  
 18                adoption of any models or reference architecture;

19                (2) an identification of activities that have not  
 20                yet been completed and that would have the most  
 21                immediate security impact; and

22                (3) a schedule to implement any planned activi-  
 23                ties.

24           (c) **CLASSIFIED ANNEX.**—Each update required  
 25          under subsection (b) may include 1 or more annexes that

1 contain classified or other sensitive information, as appro-  
2 priate.

3 (d) NATIONAL SECURITY SYSTEMS.—

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

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

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

2 (a) **DEFINITION.**—In this section, the term “informa-  
3 tion system” has the meaning given the term in section  
4 3502 of title 44, United States Code.

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

6 (1) **IN GENERAL.**—As appropriate, the Director  
7 shall issue guidance on the use of artificial intel-  
8 ligence by agencies to improve the cybersecurity of  
9 information systems.

10 (2) **CONSIDERATIONS.**—The Director and head  
11 of each agency shall consider the use and capabilities  
12 of artificial intelligence systems wherever automation  
13 is used in furtherance of the cybersecurity of infor-  
14 mation systems.

15 (3) **REPORT.**—Not later than 1 year after the  
16 date of enactment of this Act, and annually there-  
17 after until the date that is 5 years after the date of  
18 enactment of this Act, the Director shall submit to  
19 the appropriate congressional committees a report  
20 on the use of artificial intelligence to further the cy-  
21 bersecurity of information systems.

22 (c) **COMPTROLLER GENERAL REPORTS.**—

23 (1) **IN GENERAL.**—Not later than 2 years after  
24 the date of enactment of this Act, the Comptroller  
25 General of the United States shall submit to the ap-  
26 propriate congressional committees a report on the

1 risks to the privacy of individuals and the cybersecu-  
2 rity of information systems associated with the use  
3 by Federal agencies of artificial intelligence systems  
4 or capabilities.

5 (2) STUDY.—Not later than 2 years after the  
6 date of enactment of this Act, the Comptroller Gen-  
7 eral of the United States shall perform a study, and  
8 submit to the Committees on Homeland Security  
9 and Governmental Affairs and Commerce, Science,  
10 and Transportation of the Senate and the Commit-  
11 tees on Oversight and Accountability, Homeland Se-  
12 curity, and Science, Space, and Technology of the  
13 House of Representatives a report, on the use of au-  
14 tomation, including artificial intelligence, and ma-  
15 chine-readable data across the Federal Government  
16 for cybersecurity purposes, including the automated  
17 updating of cybersecurity tools, sensors, or processes  
18 employed by agencies under paragraphs (1), (5)(C),  
19 and (8)(B) of section 3554(b) of title 44, United  
20 States Code, as amended by this Act.

21 **SEC. 15. EXTENSION OF CHIEF DATA OFFICER COUNCIL.**

22 Section 3520A(c)(2) of title 44, United States Code,  
23 is amended by striking “upon the expiration of the 2-year  
24 period that begins on the date the Comptroller General

1 submits the report under paragraph (1) to Congress” and  
 2 inserting “December 31, 2031”.

3 **SEC. 16. COUNCIL OF THE INSPECTORS GENERAL ON IN-**  
 4 **TEGRITY AND EFFICIENCY DASHBOARD.**

5 (a) DASHBOARD REQUIRED.—Section 424(e) of title  
 6 5, United States Code, is amended—

7 (1) in paragraph (2)—

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

10 (B) by redesignating subparagraph (B) as  
 11 subparagraph (C);

12 (C) by inserting after subparagraph (A)  
 13 the following:

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

19 “(5) RULE OF CONSTRUCTION.—Nothing in  
 20 this subsection shall be construed to require the pub-  
 21 lication of information that is exempted from disclo-  
 22 sure under section 552 of this title.”.

1 **SEC. 17. SECURITY OPERATIONS CENTER SHARED SERV-**  
2 **ICE.**

3 (a) BRIEFING.—Not later than 180 days after the  
4 date of enactment of this Act, the Director of the Cyberse-  
5 curity and Infrastructure Security Agency shall provide to  
6 the Committee on Homeland Security and Governmental  
7 Affairs of the Senate and the Committee on Homeland  
8 Security and the Committee on Oversight and Account-  
9 ability of the House of Representatives a briefing on—

10 (1) existing security operations center shared  
11 services;

12 (2) the capability for such shared service to  
13 offer centralized and simultaneous support to mul-  
14 tiple agencies;

15 (3) the capability for such shared service to in-  
16 tegrate with or support agency threat hunting activi-  
17 ties authorized under section 3553 of title 44,  
18 United States Code, as amended by this Act;

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

22 (5) future plans for expansion and maturation  
23 of such shared service.

24 (b) GAO REPORT.—Not less than 540 days after the  
25 date of enactment of this Act, the Comptroller General  
26 of the United States shall submit to the appropriate con-



1 gressional committees a report on Federal cybersecurity  
 2 security operations centers that—

3           (1) identifies Federal agency best practices for  
 4 efficiency and effectiveness;

5           (2) identifies non-Federal best practices used by  
 6 large entity operations centers and entities providing  
 7 operation centers as a service; and

8           (3) includes recommendations for the Cyberse-  
 9 curity and Infrastructure Security Agency and any  
 10 other relevant agency to improve the efficiency and  
 11 effectiveness of security operations centers shared  
 12 service offerings.

13 **SEC. 18. 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  
 18 Federal 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  
8           inventory required under section 3505(e);

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

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

17                  “(D) implement a single sign-on trusted  
18          identity platform for individuals accessing each  
19          public website of the agency that requires user  
20          authentication, as developed by the Adminis-  
21          trator of General Services in collaboration with  
22          the Secretary; and

23                  “(E) implement identity management con-  
24          sistent with section 504 of the Cybersecurity

Enhancement Act of 2014 (15 U.S.C. 7464),  
including multi-factor authentication, for—

“(i) remote access to a information  
system; and

“(ii) each user account with elevated  
privileges on a information system.

~~“(2) PROHIBITION.—~~

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

~~“(B) PROHIBITION.—Consistent with poli-  
cies, standards, guidelines, and directives on in-  
formation security under this subchapter, and  
except as provided under paragraph (3), the  
head of an agency may not procure, obtain,  
renew a contract to procure or obtain in any  
amount, notwithstanding section 1905 of title  
41, United States Code, or use an Internet of  
things device if the Chief Information Officer of  
the agency determines during a review required  
under section 11319(b)(1)(C) of title 40 of a  
contract for an Internet of things device that  
the use of the device prevents compliance with  
the standards and guidelines developed under  
section 4 of the IoT Cybersecurity Improvement~~

1           Act (~~15 U.S.C. 278g-3b~~) with respect to the  
2           device.

3           ~~“(3) EXCEPTION.—~~The requirements under  
4           paragraph (1) shall not apply to a information sys-  
5           tem for which—

6                     ~~“(A) the head of the agency, without dele-~~  
7                     ~~gation, has certified to the Director with par-~~  
8                     ~~ticularity that—~~

9                             ~~“(i) operational requirements articu-~~  
10                            ~~lated in the certification and related to the~~  
11                            ~~information system would make it exces-~~  
12                            ~~sively burdensome to implement the cyber-~~  
13                            ~~security requirement;~~

14                           ~~“(ii) the cybersecurity requirement is~~  
15                            ~~not necessary to secure the information~~  
16                            ~~system or agency information stored on or~~  
17                            ~~transiting it; and~~

18                           ~~“(iii) the agency has taken all nec-~~  
19                            ~~essary steps to secure the information sys-~~  
20                            ~~tem and agency information stored on or~~  
21                            ~~transiting it; and~~

22                           ~~“(B) the head of the agency has submitted~~  
23                            ~~the certification described in subparagraph (A)~~  
24                            ~~to the appropriate congressional committees~~  
25                            ~~and the authorizing committees of the agency.~~

1           “(4) DURATION OF CERTIFICATION.—

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

8           “~~(B)~~ RENEWAL.—Upon the expiration of a  
9           certification of an agency under paragraph ~~(3)~~,  
10          the head of the agency may submit an addi-  
11          tional certification in accordance with that  
12          paragraph.

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

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

19          “(B) to affect the standards or process of  
20          the National Institute of Standards and Tech-  
21          nology;

22          “(C) to affect the requirement under sec-  
23          tion ~~3553~~(a)(4); or

24          “(D) to discourage continued improve-  
25          ments and advancements in the technology;

1 standards, policies, and guidelines used to pro-  
 2 mote Federal information security.

3 ~~“(g) EXCEPTION.—~~

4 ~~“(1) REQUIREMENTS.—~~The requirements under  
 5 subsection (f)(1) shall not apply to—

6 ~~“(A) the Department of Defense;~~

7 ~~“(B) a national security system; or~~

8 ~~“(C) an element of the intelligence commu-~~  
 9 ~~nity.~~

10 ~~“(2) PROHIBITION.—~~The prohibition under  
 11 subsection (f)(2) shall not apply to—

12 ~~“(A) Internet of things devices that are or~~  
 13 ~~comprise a national security system;~~

14 ~~“(B) national security systems; or~~

15 ~~“(C) a procured Internet of things device~~  
 16 ~~described in subsection (f)(2)(B) that the Chief~~  
 17 ~~Information Officer of an agency determines~~  
 18 ~~is—~~

19 ~~“(i) necessary for research purposes;~~

20 ~~or~~

21 ~~“(ii) secured using alternative and ef-~~  
 22 ~~fective methods appropriate to the function~~  
 23 ~~of the Internet of things device.”.~~

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

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

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

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

9           “(E) with respect to any exemption from  
 10 the requirements of subsection (f)(3) that is ef-  
 11 fective on the date of submission of the report,  
 12 the number of information systems that have  
 13 received an exemption from those require-  
 14 ments.”.

15       (c) DURATION OF CERTIFICATION EFFECTIVE  
 16 DATE.—Paragraph (3) of section 3554(f) of title 44,  
 17 United States Code, as added by this Act, shall take effect  
 18 on the date that is 1 year after the date of enactment  
 19 of this Act.

20       (d) FEDERAL CYBERSECURITY ENHANCEMENT ACT  
 21 OF 2015 UPDATE.—Section 222(3)(B) of the Federal Cy-  
 22 bersecurity Enhancement Act of 2015 (6 U.S.C.  
 23 1521(3)(B)) is amended by inserting “and the Committee  
 24 on Oversight and Accountability” before “of the House of  
 25 Representatives.”

1 **SEC. 19. FEDERAL CHIEF INFORMATION SECURITY OFFI-**  
 2 **CER.**

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

6 **“§ 3617. Federal chief information security officer**

7 **“(a) ESTABLISHMENT.**—There is established a Fed-  
 8 eral Chief Information Security Officer, who shall serve  
 9 in—

10 **“(1)** the Office of the Federal Chief Informa-  
 11 tion Officer of the Office of Management and Budg-  
 12 et; and

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

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

16 **“(c) OMB DUTIES.**—The Federal Chief Information  
 17 Security Officer shall report to the Federal Chief Informa-  
 18 tion Officer and assist the Federal Chief Information Offi-  
 19 cer in carrying out—

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

21 **“(2)** every function assigned to the Director  
 22 under title II of the E-Government Act of 2002 (44  
 23 U.S.C. 3501 note; Public Law 107-347);

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



1           “(4) other Federal cybersecurity initiatives de-  
2           termined by the Federal Chief Information Officer.

3           “(d) ~~ADDITIONAL DUTIES.~~—The Federal Chief In-  
4           formation Security Officer shall—

5           “(1) support the Federal Chief Information Of-  
6           ficer in overseeing and implementing Federal cyber-  
7           security under the E-Government Act of 2002 (Pub-  
8           lic Law 107-347, 116 Stat. 2899) and other rel-  
9           evant statutes in a manner consistent with law; and

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

13          “(e) ~~COORDINATION WITH ONCD.~~—The Federal  
14          Chief Information Security Officer shall support initiatives  
15          determined by the Federal Chief Information Officer nec-  
16          essary to coordinate with the Office of the National Cyber  
17          Director.”.

18          “(b) ~~NATIONAL CYBER DIRECTOR DUTIES.~~—Section  
19          1752 of the William M. (Mac) Thornberry National De-  
20          fense Authorization Act for Fiscal Year 2021 (6 U.S.C.  
21          1500) is amended—

22                 (1) by redesignating subsection (g) as sub-  
23                 section (h); and

24                 (2) by inserting after subsection (f) the fol-  
25                 lowing:

1       “(g) ~~SENIOR FEDERAL CYBERSECURITY OFFICER.—~~  
 2     The Federal Chief Information Security Officer appointed  
 3     by the President under section 3617 of title 44, United  
 4     States Code, shall be a senior official within the Office  
 5     and carry out duties applicable to the protection of infor-  
 6     mation technology (as defined in section 11101 of title 40,  
 7     United States Code), including initiatives determined by  
 8     the Director necessary to coordinate with the Office of the  
 9     Federal Chief Information Officer.”.

10       (e) ~~TREATMENT OF INCUMBENT.—~~The individual  
 11     serving as the Federal Chief Information Security Officer  
 12     appointed by the President as of the date of the enactment  
 13     of this Act may serve as the Federal Chief Information  
 14     Security Officer under section 3617 of title 44, United  
 15     States Code, as added by this Act, beginning on the date  
 16     of enactment of this Act, without need for a further or  
 17     additional appointment under such section.

18       (d) ~~CLERICAL AMENDMENT.—~~The table of sections  
 19     for chapter 36 of title 44, United States Code, is amended  
 20     by adding at the end the following:

“Sec. 3617. Federal chief information security officer”.

21     **SEC. 20. RENAMING OFFICE OF THE FEDERAL CHIEF IN-**  
 22                                   **FORMATION OFFICER.**

23       (a) ~~DEFINITIONS.—~~

24               (1) ~~IN GENERAL.—~~Section 3601 of title 44,  
 25     United States Code, is amended—

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

2 (B) by redesignating paragraphs (2)  
3 through (8) as paragraphs (1) through (7), re-  
4 spectively.

5 (2) CONFORMING AMENDMENTS.—

6 (A) TITLE 10.—Section 2222(i)(6) of title  
7 10, United States Code, is amended by striking  
8 “section 3601(4)” and inserting “section  
9 3601”.

10 (B) NATIONAL SECURITY ACT OF 1947.—  
11 Section 506D(k)(1) of the National Security  
12 Act of 1947 (50 U.S.C. 3100(k)(1)) is amended  
13 by striking “section 3601(4)” and inserting  
14 “section 3601”.

15 (b) OFFICE OF ELECTRONIC GOVERNMENT.—Section  
16 3602 of title 44, United States Code, is amended—

17 (1) in the heading, by striking “**OFFICE OF**  
18 **ELECTRONIC GOVERNMENT**” and inserting “**OF-**  
19 **FICE OF THE FEDERAL CHIEF INFORMATION**  
20 **OFFICER**”;

21 (2) in subsection (a), by striking “Office of  
22 Electronic Government” and inserting “Office of the  
23 Federal Chief Information Officer”;

(3) in subsection (b), by striking “an Administrator” and inserting “a Federal Chief Information Officer”;

(4) in subsection (c), in the matter preceding paragraph (1), by striking “The Administrator” and inserting “The Federal Chief Information Officer”;

(5) in subsection (d), in the matter preceding paragraph (1), by striking “The Administrator” and inserting “The Federal Chief Information Officer”;

(6) in subsection (e), in the matter preceding paragraph (1), by striking “The Administrator” and inserting “The Federal Chief Information Officer”;

(7) in subsection (f)—

(A) in the matter preceding paragraph (1), by striking “the Administrator” and inserting “the Federal Chief Information Officer”;

(B) in paragraph (16), by striking “the Office of Electronic Government” and inserting “the Office of the Federal Chief Information Officer”; and

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

(c) CHIEF INFORMATION OFFICERS COUNCIL.—Section 3603 of title 44, United States Code, is amended—

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

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

9           (3) in subsection (f)—

10           (A) in paragraph (3), by striking “the Ad-  
 11       ministrator” and inserting “the Federal Chief  
 12       Information Officer”; and

13           (B) in paragraph (5), by striking “the Ad-  
 14       ministrator” and inserting “the Federal Chief  
 15       Information Officer”.

16       (d) ~~E-GOVERNMENT FUND.~~—Section 3604 of title  
 17   44, United States Code, is amended—

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

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

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

4           ~~(e) PROGRAM TO ENCOURAGE INNOVATIVE SOLU-~~  
 5           ~~TIONS TO ENHANCE ELECTRONIC GOVERNMENT SERV-~~  
 6           ~~ICES AND PROCESSES.—Section 3605 of title 44, United~~  
 7           ~~States Code, is amended—~~

8           (1) in subsection (a), by striking “The Adminis-

9           trator” and inserting “The Federal Chief Informa-

10          tion Officer”;

11          (2) in subsection (b), by striking “, the Admin-

12          istrator,” and inserting “, the Federal Chief Infor-

13          mation Officer,”; and

14          ~~(3)~~ in subsection (c)—

15               ~~(A) in paragraph (1)—~~

16                   (i) by striking “The Administrator”

17                   and inserting “The Federal Chief Informa-

18                   tion Officer”; and

19                   (ii) by striking “proposals submitted

20                   to the Administrator” and inserting “pro-

21                   posals submitted to the Federal Chief In-

22                   formation Officer”;

23               ~~(B) in paragraph (2)(B), by striking “the~~

24               ~~Administrator” and inserting “the Federal~~

25               ~~Chief Information Officer”; and~~

1                   (C) in paragraph (4), by striking “the Ad-  
 2                   ministrator” and inserting “the Federal Chief  
 3                   Information Officer”.

4           (f) ~~E-GOVERNMENT REPORT.~~—Section 3606 of title  
 5   44, United States Code, is amended in the section heading  
 6   by striking “**E-Government**” and inserting “**An-**  
 7   **nual**”.

8           (g) ~~TREATMENT OF INCUMBENT.~~—The individual  
 9   serving as the Administrator of the Office of Electronic  
 10   Government under section 3602 of title 44, United States  
 11   Code, as of the date of the enactment of this Act, may  
 12   continue to serve as the Federal Chief Information Officer  
 13   commencing as of that date, without need for a further  
 14   or additional appointment under such section.

15          (h) ~~TECHNICAL AND CONFORMING AMENDMENTS.~~—  
 16   The table of sections for chapter 36 of title 44, United  
 17   States Code, is amended—

18               (1) by striking the item relating to section 3602  
 19               and inserting the following:

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

20               (2) in the item relating to section 3606, by  
 21               striking “E-Government” and inserting “Annual”.

22          (i) ~~REFERENCES.~~—

23               (1) ~~ADMINISTRATOR.~~—Any reference to the Ad-  
 24               ministrator of the Office of Electronic Government  
 25               in any law, regulation, map, document, record, or

1 other paper of the United States shall be deemed to  
 2 be a reference to the Federal Chief Information Offi-  
 3 cer.

4 (2) OFFICE OF ELECTRONIC GOVERNMENT.—  
 5 Any reference to the Office of Electronic Govern-  
 6 ment in any law, regulation, map, document, record,  
 7 or other paper of the United States shall be deemed  
 8 to be a reference to the Office of the Federal Chief  
 9 Information Officer.

10 **SEC. 21. RULES OF CONSTRUCTION.**

11 (a) AGENCY ACTIONS.—Nothing in this Act, or an  
 12 amendment made by this Act, shall be construed to au-  
 13 thorize the head of an agency to take an action that is  
 14 not authorized by this Act, an amendment made by this  
 15 Act, or existing law.

16 (b) PROTECTION OF RIGHTS.—Nothing in this Act,  
 17 or an amendment made by this Act, shall be construed  
 18 to permit the violation of the rights of any individual pro-  
 19 tected by the Constitution of the United States, including  
 20 through censorship of speech protected by the Constitu-  
 21 tion of the United States or unauthorized surveillance.

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

23 (a) *SHORT TITLE.*—*This Act may be cited as the “Cy-*  
 24 *bersecurity Act of 2023”.*



1       (b) *TABLE OF CONTENTS.—The table of contents for*  
 2 *this Act is as follows:*

*Sec. 1. Short title; table of contents.*

***TITLE I—FEDERAL INFORMATION SECURITY MODERNIZATION ACT  
OF 2023***

*Sec. 101. Short title.*

*Sec. 102. Definitions.*

*Sec. 103. Amendments to title 44.*

*Sec. 104. Amendments to subtitle III of title 40.*

*Sec. 105. Actions to enhance Federal incident transparency.*

*Sec. 106. Additional guidance to agencies on FISMA updates.*

*Sec. 107. Agency requirements to notify private sector entities impacted by incidents.*

*Sec. 108. Mobile security briefings.*

*Sec. 109. Data and logging retention for incident response.*

*Sec. 110. CISA agency liaisons.*

*Sec. 111. Federal penetration testing policy.*

*Sec. 112. Vulnerability disclosure policies.*

*Sec. 113. Implementing zero trust architecture.*

*Sec. 114. Automation and artificial intelligence.*

*Sec. 115. Extension of chief data officer council.*

*Sec. 116. Council of the inspectors general on integrity and efficiency dashboard.*

*Sec. 117. Security operations center shared service.*

*Sec. 118. Federal cybersecurity requirements.*

*Sec. 119. Federal chief information security officer.*

*Sec. 120. Renaming office of the Federal Chief Information Officer.*

*Sec. 121. Rules of construction.*

***TITLE II—RURAL HOSPITAL CYBERSECURITY ENHANCEMENT ACT***

*Sec. 201. Short title.*

*Sec. 202. Definitions.*

*Sec. 203. Rural hospital cybersecurity workforce development strategy.*

*Sec. 204. Instructional materials for rural hospitals.*

*Sec. 205. No additional funds.*

3 ***TITLE I—FEDERAL INFORMA-***  
 4 ***TION SECURITY MODERNIZA-***  
 5 ***TION ACT OF 2023***

6 ***SEC. 101. SHORT TITLE.***

7       *This title may be cited as the “Federal Information*  
 8 *Security Modernization Act of 2023”.*

1 **SEC. 102. DEFINITIONS.**

2 *In this title, unless otherwise specified:*

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

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

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

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

13 (C) *the Committee on Homeland Security of*  
14 *the House of Representatives.*

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

18 (4) *CONTRACTOR.*—*The term “contractor” has*  
19 *the meaning given the term in section 3591 of title*  
20 *44, United States Code, as added by this title.*

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

23 (6) *FEDERAL INFORMATION SYSTEM.*—*The term*  
24 *“Federal information system” has the meaning give*  
25 *the term in section 3591 of title 44, United States*  
26 *Code, as added by this title.*

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

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

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

12          (10) *THREAT HUNTING*.—The term “threat hunt-  
13          ing” means proactively and iteratively searching sys-  
14          tems for threats and vulnerabilities, including threats  
15          or vulnerabilities that may evade detection by auto-  
16          mated threat detection systems.

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

22   **SEC. 103. AMENDMENTS TO TITLE 44.**

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

25               (1) in section 3504—

1                   (A) in subsection (a)(1)(B)—

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

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

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

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

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

13                  (B) in subsection (g)—

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

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

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

22                  “(2) in consultation with the National Cyber Di-  
23                  rector, oversee the implementation of policies, prin-  
24                  ciples, standards, and guidelines on security, of infor-

1        *mation collected or maintained by or for agencies;*  
 2        *and”;*

3            *(2) in section 3505—*

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

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

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

13                            *(i) in subparagraph (B)—*

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

19                                    *(II) by striking “and” at the end;*

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

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

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

4           (3) in section 3506—

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

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

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

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

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

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

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

4           “(2) The Chief Privacy Officer of each agency shall—  
5           “(A) serve in a central leadership position with-  
6           in the agency;

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

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

12          “(3) A privacy officer of an agency established under  
13          a statute enacted before the date of enactment of the Federal  
14          Information Security Modernization Act of 2023 may carry  
15          out the responsibilities under this subsection for the agen-  
16          cy.”; and

17          (4) in section 3513—

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

20                  (B) by inserting after subsection (b) the fol-  
21                  lowing:

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

1       (b) *SUBCHAPTER II DEFINITIONS.*—

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

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

7                       (B) *by inserting after paragraph (1) the fol-*  
8       *lowing:*

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

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

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

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



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

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

5       “(9) The term ‘penetration test’—

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

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

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

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

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

25              (2) CONFORMING AMENDMENTS.—

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

6           (B) *TITLE 10.*—

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

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

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

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

23           (C) *HIGH-PERFORMANCE COMPUTING ACT*  
 24           *OF 1991.*—*Section 207(a) of the High-Perform-*  
 25           *ance Computing Act of 1991 (15 U.S.C. 5527(a))*

1       is       amended       by       striking       “section  
 2       3552(b)(6)(A)(i)”       and       inserting       “section  
 3       3552(b)(8)(A)(i)”.

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

10              (E) *NATIONAL DEFENSE AUTHORIZATION*  
 11       *ACT FOR FISCAL YEAR 2013*.—Section  
 12       933(e)(1)(B) of the *National Defense Authoriza-*  
 13       *tion Act for Fiscal Year 2013 (10 U.S.C. 2224*  
 14       *note)* is amended by striking “section  
 15       3542(b)(2)” and inserting “section 3552(b)”.

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

21                   (i) in section 806(e)(5) (10 U.S.C.  
 22                   2304 note), by striking “section 3542(b)”  
 23                   and inserting “section 3552(b)”;

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

4                   (iii) in section 932(b)(2) (10 U.S.C.  
5                   2224 note), by striking “section 3542(b)(2)”  
6                   and inserting “section 3552(b)”.

7                   (G) *E-GOVERNMENT ACT OF 2002*.—Section  
8                   301(c)(1)(A) of the *E-Government Act of 2002*  
9                   (44 U.S.C. 3501 note) is amended by striking  
10                  “section 3542(b)(2)” and inserting “section  
11                  3552(b)”.

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

16                   (i) in subsection (a)(2), by striking  
17                   “section 3552(b)(6)” and inserting “section  
18                   3552(b)”; and

19                   (ii) in subsection (f)—

20                   (I) in paragraph (2), by striking  
21                   “section 3552(b)(2)” and inserting  
22                   “section 3552(b)”; and

23                   (II) in paragraph (5), by striking  
24                   “section 3532(b)(5)” and inserting  
25                   “section 3552(b)”.

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

3           (1) *in section 3551—*

4               (A) *in paragraph (4), by striking “diagnose*  
5 *and improve” and inserting “integrate, deliver,*  
6 *diagnose, and improve”;*

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

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

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

12                   “(7) *recognize that each agency has specific mis-*  
13 *sion requirements and, at times, unique cybersecurity*  
14 *requirements to meet the mission of the agency;*

15                   “(8) *recognize that each agency does not have the*  
16 *same resources to secure agency systems, and an agen-*  
17 *cy should not be expected to have the capability to se-*  
18 *cure the systems of the agency from advanced adver-*  
19 *saries alone; and*

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

23           (2) *in section 3553—*

24               (A) *in subsection (a)—*

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

3                   (ii) in paragraph (6), by striking the  
4                   period at the end and inserting “; and”;  
5                   and

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

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

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

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

20                  (B) in subsection (b)—

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

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

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

3 *(iii) by redesignating paragraphs (8)*  
 4 *and (9) as paragraphs (10) and (11), re-*  
 5 *spectively; and*

6 *(iv) by inserting after paragraph (7)*  
 7 *the following:*

8 *“(8) expeditiously seeking opportunities to re-*  
 9 *duce costs, administrative burdens, and other barriers*  
 10 *to information technology security and modernization*  
 11 *for agencies, including through shared services for cy-*  
 12 *bersecurity capabilities identified as appropriate by*  
 13 *the Director, in coordination with the Director of the*  
 14 *Cybersecurity and Infrastructure Security Agency*  
 15 *and other agencies as appropriate;”;*

16 *(C) in subsection (c)—*

17 *(i) in the matter preceding paragraph*  
 18 *(1)—*

19 *(I) by striking “each year” and*  
 20 *inserting “each year during which*  
 21 *agencies are required to submit reports*  
 22 *under section 3554(c)”;*

23 *(II) by inserting “, which shall be*  
 24 *unclassified but may include 1 or more*  
 25 *annexes that contain classified or other*

1                    *sensitive information, as appropriate”*  
 2                    *after “a report”; and*

3                    *(III) by striking “preceding year”*  
 4                    *and inserting “preceding 2 years”;*

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

6                    *(iii) by redesignating paragraphs (2),*  
 7                    *(3), and (4) as paragraphs (1), (2), and (3),*  
 8                    *respectively;*

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

11                    *(v) by inserting after paragraph (3),*  
 12                    *as so redesignated, the following:*

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

16                    *(D) in subsection (h)—*

17                    *(i) in paragraph (2)—*

18                    *(I) in subparagraph (A), by in-*  
 19                    *serting “and the National Cyber Direc-*  
 20                    *tor” after “in coordination with the*  
 21                    *Director”; and*

22                    *(II) in subparagraph (D), by in-*  
 23                    *serting “, the National Cyber Direc-*  
 24                    *tor,” after “notify the Director”; and*



1                   (ii) in paragraph (3)(A)(iv), by insert-  
2                   ing “, the National Cyber Director,” after  
3                   “the Secretary provides prior notice to the  
4                   Director”;

5                   (E) by amending subsection (i) to read as  
6                   follows:

7                   “(i) *FEDERAL RISK ASSESSMENT.*—On an ongoing  
8                   and continuous basis, the Director of the Cybersecurity and  
9                   Infrastructure Security Agency shall assess the Federal risk  
10                  posture using any available information on the cybersecu-  
11                  rity posture of agencies, and brief the Director and National  
12                  Cyber Director on the findings of such assessment, includ-  
13                  ing—

14                  “(1) the status of agency cybersecurity remedial  
15                  actions for high value assets described in section  
16                  3554(b)(7);

17                  “(2) any vulnerability information relating to  
18                  the systems of an agency that is known by the agency;

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

21                  “(4) evaluation of penetration testing performed  
22                  under section 3559A;

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

25                  “(6) evaluation of agency threat hunting results;

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

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

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

7           “(10) *relevant reports from inspectors general of*  
8           *agencies and the Government Accountability Office;*  
9           *and*

10          “(11) *any other information the Director of the*  
11          *Cybersecurity and Infrastructure Security Agency de-*  
12          *termines relevant.”; and*

13                       *(F) by adding at the end the following:*

14          “(m) *DIRECTIVES.—*

15               “(1) *EMERGENCY DIRECTIVE UPDATES.—If the*  
16               *Secretary issues an emergency directive under this*  
17               *section, the Director of the Cybersecurity and Infra-*  
18               *structure Security Agency shall submit to the Direc-*  
19               *tor, the National Cyber Director, the Committee on*  
20               *Homeland Security and Governmental Affairs of the*  
21               *Senate, and the Committees on Oversight and Ac-*  
22               *countability and Homeland Security of the House of*  
23               *Representatives an update on the status of the imple-*  
24               *mentation of the emergency directive at agencies not*  
25               *later than 7 days after the date on which the emer-*

1     *gency directive requires an agency to complete a re-*  
 2     *quirement specified by the emergency directive, and*  
 3     *every 30 days thereafter until—*

4             *“(A) the date on which every agency has*  
 5             *fully implemented the emergency directive;*

6             *“(B) the Secretary determines that an emer-*  
 7             *gency directive no longer requires active report-*  
 8             *ing from agencies or additional implementation;*  
 9             *or*

10            *“(C) the date that is 1 year after the*  
 11            *issuance of the directive.*

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

1           “(A) the date on which every agency has  
2           fully implemented the binding operational direc-  
3           tive;

4           “(B) the Secretary determines that a bind-  
5           ing operational directive no longer requires ac-  
6           tive reporting from agencies or additional imple-  
7           mentation; or

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

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

21                 “(A) has not completed a requirement speci-  
22                 fied by an emergency directive; or

23                 “(B) has not implemented a binding oper-  
24                 ational directive.

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

3               “(1) *CONDUCT OF REVIEW.*—*Not less frequently*  
4 *than once every 3 years, the Director of the Office of*  
5 *Management and Budget shall review the efficacy of*  
6 *the guidance and policy promulgated by the Director*  
7 *in reducing cybersecurity risks, including a consider-*  
8 *ation of reporting and compliance burden on agen-*  
9 *cies.*

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

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

21              “(o) *AUTOMATED STANDARD IMPLEMENTATION*  
22 *VERIFICATION.*—*When the Director of the National Insti-*  
23 *tute of Standards and Technology issues a proposed stand-*  
24 *ard or guideline pursuant to paragraphs (2) or (3) of sec-*  
25 *tion 20(a) of the National Institute of Standards and Tech-*

1 *nology Act (15 U.S.C. 278g–3(a)), the Director of the Na-*  
 2 *tional Institute of Standards and Technology shall consider*  
 3 *developing and, if appropriate and practical, develop speci-*  
 4 *fications to enable the automated verification of the imple-*  
 5 *mentation of the controls.*

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

13 (3) *in section 3554—*

14 (A) *in subsection (a)—*

15 (i) *in paragraph (1)—*

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

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

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

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

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

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

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

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

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

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

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

3                   “(III) information provided to the  
4                   agency through the vulnerability dis-  
5                   closure program of the agency under  
6                   section 3559B;

7                   “(IV) incidents; and

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

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

17                  “(viii) assessing the consequences of po-  
18                  tential incidents occurring on agency sys-  
19                  tems that would impact systems at other  
20                  agencies, including due to interconnectivity  
21                  between different agency systems or oper-  
22                  ational reliance on the operations of the sys-  
23                  tem or data in the system;”;

24                  (III) in subparagraph (B), as so  
25                  redesignated, in the matter preceding



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

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

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

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

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

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

18 *“(i) upon request, to the inspector gen-*  
 19 *eral of the agency or the Comptroller Gen-*  
 20 *eral of the United States; and*

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

25 *“(I) the Director;*

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

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

6           (ii) in paragraph (2)—

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

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

18          (iii) in paragraph (3)(A)—

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

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

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

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

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

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

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

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

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

1                   *(B) in subsection (b)—*

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

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

10                  *(ii) in paragraph (2)—*

11                   *(I) by striking subparagraph (B);*

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

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

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

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

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

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

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

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

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

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

19                      “(7) *a secure process for providing the status of*  
 20                      *every remedial action and unremediated identified*  
 21                      *system vulnerability of a high value asset to the Di-*  
 22                      *rector and the Director of the Cybersecurity and In-*  
 23                      *frastructure Security Agency, using automation and*  
 24                      *machine-readable data to the greatest extent prac-*  
 25                      *ticable;*”; and

1                   (vi) in paragraph (8)(C), as so redesign-  
2                   nated—

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

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

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

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

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

16                  (IV) in clause (iv), as so redesign-  
17                  nated—

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

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

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

24                  (C) in subsection (c)—

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

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

5                   “(1) *BIENNIAL REPORT*.—Not later than 2 years  
6                   after the date of enactment of the *Federal Information*  
7                   *Security Modernization Act of 2023* and not less fre-  
8                   quently than once every 2 years thereafter, using the  
9                   continuous and ongoing agency system risk assess-  
10                  ment required under subsection (a)(1)(A), the head of  
11                  each agency shall submit to the Director, the National  
12                  Cyber Director, the Director of the Cybersecurity and  
13                  Infrastructure Security Agency, the Comptroller Gen-  
14                  eral of the United States, the majority and minority  
15                  leaders of the Senate, the Speaker and minority lead-  
16                  er of the House of Representatives, the Committee on  
17                  Homeland Security and Governmental Affairs of the  
18                  Senate, the Committee on Oversight and Account-  
19                  ability of the House of Representatives, the Committee  
20                  on Homeland Security of the House of Representa-  
21                  tives, the Committee on Commerce, Science, and  
22                  Transportation of the Senate, the Committee on  
23                  Science, Space, and Technology of the House of Rep-  
24                  resentatives, and the appropriate authorization and

1        *appropriations committees of Congress a report*  
2        *that—*

3                *“(A) summarizes the agency system risk as-*  
4                *essment required under subsection (a)(1)(A);*

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

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

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

21               *“(A) shall be, to the greatest extent prac-*  
22               *ticable, in an unclassified and otherwise uncon-*  
23               *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 “**AN-**  
18           **NUAL INDEPENDENT**” and inserting “**INDE-**  
19           **PENDENT**”;

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 in-  
 10                  clude recommendations for improving the cybersecu-  
 11                  rity posture of 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  
 2           independent evaluation under subsection (b).”;  
 3           and

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

6           “(j) GUIDANCE.—

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

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

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

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

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

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

1           (5) in section 3556(a)—

2                   (A) in the matter preceding paragraph (1),  
3           by inserting “within the Cybersecurity and In-  
4           frastructure Security Agency” after “incident  
5           center”; and

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

8           (d) CONFORMING AMENDMENTS.—

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

“3555. Independent evaluation.”.

13                  (2) OMB REPORTS.—Section 226(c) of the Cy-  
14          bersecurity Act of 2015 (6 U.S.C. 1524(c)) is amend-  
15          ed—

16                   (A) in paragraph (1)(B), in the matter pre-  
17          ceding clause (i), by striking “annually there-  
18          after” and inserting “thereafter during the years  
19          during which a report is required to be sub-  
20          mitted under section 3553(c) of title 44, United  
21          States Code”; and

22                   (B) in paragraph (2)(B), in the matter pre-  
23          ceding clause (i)—

24                   (i) by striking “annually thereafter”  
25          and inserting “thereafter during the years

during which a report is required to be submitted under section 3553(c) of title 44, United States Code”; and

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

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

(e) *FEDERAL SYSTEM INCIDENT RESPONSE.*—

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

*“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT  
RESPONSE*

**“§ 3591. *Definitions***

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

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

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

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

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

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

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

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

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

13          “(G) the Committee on Science, Space, and  
14          Technology of the House of Representatives;

15          “(H) the appropriate authorization and ap-  
16          propriations committees of Congress;

17          “(I) the Director;

18          “(J) the Director of the Cybersecurity and  
19          Infrastructure Security Agency;

20          “(K) the National Cyber Director;

21          “(L) the Comptroller General of the United  
22          States; and

23          “(M) the inspector general of any impacted  
24          agency.

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

3                   “(A) means—

4                           “(i) the recipient of a grant from an  
5                           agency;

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

8                           “(iii) a party to an other transaction  
9                           agreement with an agency; and

10                   “(B) includes a subawardee of an entity de-  
11                   scribed in subparagraph (A).

12           “(3) *BREACH*.—The term ‘breach’—

13                   “(A) means the compromise, unauthorized  
14                   disclosure, unauthorized acquisition, or loss of  
15                   control of personally identifiable information or  
16                   any similar occurrence; and

17                   “(B) includes any additional meaning  
18                   given the term in policies, principles, standards,  
19                   or guidelines issued by the Director.

20           “(4) *CONTRACTOR*.—The term ‘contractor’ means  
21           a prime contractor of an agency or a subcontractor  
22           of a prime contractor of an agency that creates, col-  
23           lects, stores, processes, maintains, or transmits Fed-  
24           eral information on behalf of an agency.

1           “(5) *FEDERAL INFORMATION*.—The term ‘Fed-  
 2       *eral information*’ means information created, col-  
 3       *lected, processed, maintained, disseminated, disclosed,*  
 4       *or disposed of by or for the Federal Government in*  
 5       *any medium or form.*

6           “(6) *FEDERAL INFORMATION SYSTEM*.—The term  
 7       ‘*Federal information system*’ means an information  
 8       system owned, managed, or operated by an agency, or  
 9       on behalf of an agency by a contractor, an awardee,  
 10      or another organization.

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

15          “(8) *NATIONWIDE CONSUMER REPORTING AGEN-*  
 16      *CY*.—The term ‘*nationwide consumer reporting agen-*  
 17      *cy*’ means a consumer reporting agency described in  
 18      section 603(p) of the Fair Credit Reporting Act (15  
 19      U.S.C. 1681a(p)).

20          “(9) *VULNERABILITY DISCLOSURE*.—The term  
 21      ‘*vulnerability disclosure*’ means a vulnerability iden-  
 22      tified under section 3559B.

23      **“§ 3592. Notification of breach**

24          “(a) *DEFINITION*.—In this section, the term ‘covered  
 25      breach’ means a breach—



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

3           “(2) the result of which the head of an agency  
4       determines that notifying potentially affected individ-  
5       uals is necessary pursuant to subsection (b)(1), re-  
6       gardless of whether—

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

9           “(B) the notification is delayed under sub-  
10      section (d).

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

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

21           “(A) the nature and sensitivity of the per-  
22       sonally identifiable information affected by the  
23       breach;

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

4                   “(C) the type of breach; and

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

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

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

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

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

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

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

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

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

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

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

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

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

17          “(d) *DELAY OF NOTIFICATION.*—

18                 “(1) *IN GENERAL.*—The head of an agency, in  
19                 coordination with the Director and the National  
20                 Cyber Director, and as appropriate, the Attorney  
21                 General, the Director of National Intelligence, or the  
22                 Secretary of Homeland Security, may delay a notifi-  
23                 cation required under subsection (b) or (e) if the noti-  
24                 fication would—

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

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

5           “(C) reveal sensitive sources and methods;

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

7           “(E) hamper security remediation actions.

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

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

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

1 “(f) *DELAY OF NOTIFICATION REPORT.*—

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

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

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

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

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

1       *the agency discovers the covered breach give notice of*  
 2       *the breach, which may be provided electronically, to—*

3               “(A) *each congressional committee described*  
 4               *in section 3554(c)(1); and*

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

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

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

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

21               “(C) *a description of any circumstances ne-*  
 22               *cessitating a delay in providing notice to indi-*  
 23               *viduals affected by the covered breach in accord-*  
 24               *ance with subsection (d); and*

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

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

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

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

12          “(C) *the appropriations committees of Con-*  
 13          *gress;*

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

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

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

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

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

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

3               “(1) *limit—*

4                       “(A) *the authority of the Director to issue*  
 5                       *guidance relating to notifications of, or the head*  
 6                       *of an agency to notify individuals potentially af-*  
 7                       *ected by, breaches that are not determined to be*  
 8                       *covered breaches or major incidents;*

9                       “(B) *the authority of the Director to issue*  
 10                      *guidance relating to notifications and reporting*  
 11                      *of breaches, covered breaches, or major incidents;*

12                      “(C) *the authority of the head of an agency*  
 13                      *to provide more information than required under*  
 14                      *subsection (b) when notifying individuals poten-*  
 15                      *tially affected by a breach;*

16                      “(D) *the timing of incident reporting or the*  
 17                      *types of information included in incident reports*  
 18                      *provided, pursuant to this subchapter, to—*

19                               “(i) *the Director;*

20                               “(ii) *the National Cyber Director;*

21                               “(iii) *the Director of the Cybersecurity*  
 22                               *and Infrastructure Security Agency; or*

23                               “(iv) *any other agency;*



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

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

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

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

11                  “(2) limit or supersede any existing privacy pro-  
12                  tections in existing law.

13   **“§ 3593. Congressional and Executive Branch reports**  
14           **on major incidents**

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

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

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

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

24                   “(4) the Committee on Commerce, Science, and  
25                   Transportation of the Senate;

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

3           “(6) *the Committee on Homeland Security of the*  
4           *House of Representatives;*

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

7           “(8) *the appropriate authorization and appro-*  
8           *priations committees of Congress*

9           “(b) *INITIAL NOTIFICATION.—*

10           “(1) *IN GENERAL.—Not later than 72 hours after*  
11           *an agency has a reasonable basis to conclude that a*  
12           *major incident occurred, the head of the agency im-*  
13           *pacted by the major incident shall submit to the ap-*  
14           *propriate reporting entities a written notification,*  
15           *which may be submitted electronically and include 1*  
16           *or more annexes that contain classified or other sen-*  
17           *sitive information, as appropriate.*

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

23           “(A) *A summary of the information avail-*  
24           *able about the major incident, including how the*

1        *major incident occurred and the threat causing*  
2        *the major incident.*

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

6                *“(i) the breach was the reason the inci-*  
7        *dent was determined to be a major incident;*  
8        *and*

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

13               *“(C) A preliminary assessment of the im-*  
14       *pacts to—*

15               *“(i) the agency;*

16               *“(ii) the Federal Government;*

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

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

23               *“(D) If applicable, whether any ransom has*  
24       *been demanded or paid, or is expected to be*  
25       *paid, by any entity operating a Federal infor-*

1            *mation system or with access to Federal infor-*  
 2            *mation or a Federal information system, includ-*  
 3            *ing, as available, the name of the entity demand-*  
 4            *ing ransom, the date of the demand, and the*  
 5            *amount and type of currency demanded, unless*  
 6            *disclosure of such information will disrupt an*  
 7            *active Federal law enforcement or national secu-*  
 8            *rity operation.*

9            “(c) *SUPPLEMENTAL UPDATE.*—*Within a reasonable*  
 10          *amount of time, but not later than 30 days after the date*  
 11          *on which the head of an agency submits a written notifica-*  
 12          *tion under subsection (a), the head of the agency shall pro-*  
 13          *vide to the appropriate congressional entities an unclassi-*  
 14          *fied and written update, which may include 1 or more an-*  
 15          *nexes that contain classified or other sensitive information,*  
 16          *as appropriate, on the major incident, based on informa-*  
 17          *tion available to agency officials as of the date on which*  
 18          *the agency provides the update, on—*

19                “(1) *system vulnerabilities relating to the major*  
 20          *incident, where applicable, means by which the major*  
 21          *incident occurred, the threat causing the major inci-*  
 22          *dent, where applicable, and impacts of the major inci-*  
 23          *dent to—*

24                “(A) *the agency;*

1           “(B) other Federal agencies, Congress, or  
2           the judicial branch;

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

6           “(D) the civil liberties, public confidence,  
7           privacy, or public health and safety of the people  
8           of the United States;

9           “(2) the status of compliance of the affected Fed-  
10          eral information system with applicable security re-  
11          quirements at the time of the major incident;

12          “(3) if the major incident involved a breach, a  
13          description of the affected information, an estimate of  
14          the number of individuals potentially impacted, and  
15          any assessment to the risk of harm to such individ-  
16          uals;

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

21          “(5) the detection, response, and remediation ac-  
22          tions of the agency, including any support provided  
23          by the Cybersecurity and Infrastructure Security  
24          Agency under section 3594(d), if applicable.

1       “(d) *ADDITIONAL UPDATE.*—If the head of an agency,  
 2   the Director, or the National Cyber Director determines that  
 3   there is any significant change in the understanding of the  
 4   scope, scale, or consequence of a major incident for which  
 5   the head of the agency submitted a written notification and  
 6   update under subsections (b) and (c), the head of the agency  
 7   shall submit to the appropriate congressional entities a  
 8   written update that includes information relating to the  
 9   change in understanding.

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

15       “(f) *REPORT DELIVERY.*—

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

18                       “(A) shall be submitted in an electronic for-  
 19   mat; and

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

21       “(2) *CLASSIFICATION STATUS.*—Any written no-  
 22   tification or update required to be submitted under  
 23   this section—

24                       “(A) shall be—

25                               “(i) unclassified; and

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

4                   “(B) may include classified annexes, as ap-  
5                   propriate.

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

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

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

17                       “(A) include, at a minimum—

18                               “(i) the full contents of the written no-  
19                               tification or update;

20                               “(ii) the identity of the reporting agen-  
21                               cy; and

22                               “(iii) the date of submission; and

23                               “(iv) a list of the recipient congres-  
24                               sional entities; and

1                   “(B) be made available upon request to the  
 2                   majority and minority leaders of the Senate, the  
 3                   Speaker and minority leader of the House of  
 4                   Representatives, the Committee on Homeland Se-  
 5                   curity and Governmental Affairs of the Senate,  
 6                   and the Committee on Oversight and Account-  
 7                   ability of the House of Representatives.

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

14                  “(1) the majority and minority leaders of the  
 15                  Senate;

16                  “(2) the Speaker and minority leader of the  
 17                  House of Representatives;

18                  “(3) the appropriations committees of Congress;

19                  “(4) the appropriate authorization committees of  
 20                  Congress;

21                  “(5) the Committee on Homeland Security and  
 22                  Governmental Affairs of the Senate;

23                  “(6) the Select Committee on Intelligence of the  
 24                  Senate;



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

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

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

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

12           “(2) *be reported to Congress under the process es-*  
13           *tablished under section 3592(g).*

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

16           “(1) *limit—*

17           “(A) *the ability of an agency to provide ad-*  
18           *ditional reports or briefings to Congress;*

19           “(B) *Congress from requesting additional*  
20           *information from agencies through reports, brief-*  
21           *ings, or other means;*

22           “(C) *any congressional reporting require-*  
23           *ments of agencies under any other law; or*

24           “(2) *limit or supersede any privacy protections*  
25           *under any other law.*

1 **“§ 3594. Government information sharing and inci-**  
 2 **dent response**

3 “(a) *IN GENERAL.*—

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

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

17 “(A) a full description of the incident, in-  
 18 cluding—

19 “(i) all indicators of compromise and  
 20 tactics, techniques, and procedures;

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

25 “(iii) information that would support  
 26 enabling defensive measures; and

1                   “(iv) other information that may assist  
2                   in identifying other victims;

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

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

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

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

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

17                  “(3) INFORMATION SHARING.—The Director of  
18                  the Cybersecurity and Infrastructure Security Agency  
19                  shall—

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

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

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

3                   “(I) impacted by the incident;

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

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

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

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

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

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

18                  “(A) IN GENERAL.—Notwithstanding para-  
19                  graphs (1) and (3), each agency operating or ex-  
20                  ercising control of a national security system  
21                  shall share information about an incident that  
22                  occurs exclusively on a national security system  
23                  with the Secretary of Defense, the Director, the  
24                  National Cyber Director, and the Director of the  
25                  Cybersecurity and Infrastructure Security Agen-

1           *cy to the extent consistent with standards and*  
2           *guidelines for national security systems issued in*  
3           *accordance with law and as directed by the*  
4           *President.*

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

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

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

1 *medium or form that does not exclusively involve a national*  
 2 *security system shall coordinate with—*

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

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

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

11           “(a) *REPORTING.—*

12           “(1) *IN GENERAL.—Any contractor or awardee*  
 13 *of an agency shall report to the agency if the con-*  
 14 *tractor or awardee has a reasonable basis to conclude*  
 15 *that—*

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

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

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

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

8                *“(D) the contractor or awardee has received*  
9        *personally identifiable information, personal*  
10       *health information, or other clearly sensitive in-*  
11       *formation that is beyond the scope of the contract*  
12       *or agreement with the agency from the agency*  
13       *that the contractor or awardee is not authorized*  
14       *to receive.*

15        *“(2)        THIRD-PARTY        REPORTS        OF*  
16       *VULNERABILITIES.—Subject to the guidance issued by*  
17       *the Director pursuant to paragraph (4), any con-*  
18       *tractor or awardee of an agency shall report to the*  
19       *agency and the Cybersecurity and Infrastructure Se-*  
20       *curity Agency if the contractor or awardee has a rea-*  
21       *sonable basis to suspect or conclude that a component*  
22       *of any Federal information system operated, man-*  
23       *aged, or maintained on behalf of an agency by the*  
24       *contractor or awardee on behalf of the agency con-*  
25       *tains a security vulnerability, including a supply*

1 *chain compromise or an identified software or hard-*  
 2 *ware vulnerability, that has been reported to the con-*  
 3 *tractor or awardee by a third party, including*  
 4 *through a vulnerability disclosure program.*

5 “(3) *PROCEDURES.*—

6 “(A) *SHARING WITH CISA.*—As soon as  
 7 *practicable following a report of an incident to*  
 8 *an agency by a contractor or awardee under*  
 9 *paragraph (1), the head of the agency shall pro-*  
 10 *vide, pursuant to section 3594, information*  
 11 *about the incident to the Director of the Cyberse-*  
 12 *curity and Infrastructure Security Agency.*

13 “(B) *TIME FOR REPORTING.*—Unless a dif-  
 14 *ferent time for reporting is specified in a con-*  
 15 *tract, grant, cooperative agreement, or other*  
 16 *transaction agreement, a contractor or awardee*  
 17 *shall—*

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

24 “(ii) *make a report required under*  
 25 *paragraph (2) within a reasonable time, but*



1           *not later than 90 days after the date on*  
2           *which the contractor or awardee has reason-*  
3           *able basis to suspect or conclude that the*  
4           *criteria under paragraph (2) have been met.*

5           “(C) *PROCEDURES.*—*Following a report of*  
6           *a breach or incident to an agency by a con-*  
7           *tractor or awardee under paragraph (1), the*  
8           *head of the agency, in consultation with the con-*  
9           *tractor or awardee, shall carry out the applicable*  
10          *requirements under sections 3592, 3593, and*  
11          *3594 with respect to the breach or incident.*

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

18          “(4) *GUIDANCE.*—*The Director shall issue guid-*  
19          *ance to agencies relating to the scope of vulnerabilities*  
20          *to be reported under paragraph (2), such as the min-*  
21          *imum severity of a vulnerability required to be re-*  
22          *ported or whether vulnerabilities that are already*  
23          *publicly disclosed must be reported.*

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

1           “(1) *IN GENERAL.*—Not later than 1 year after  
 2           the date of enactment of the Federal Information Se-  
 3           curity Modernization Act of 2023—

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 Federal Regulations, as appropriate, re-*  
 13                   *lating 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) NATIONAL SECURITY SYSTEMS EXEMPTION.—  
 13          *Notwithstanding any other provision of this section, a con-*  
 14          *tractor or awardee of an agency that would be required to*  
 15          *report an incident or vulnerability pursuant to this section*  
 16          *that occurs exclusively on a national security system*  
 17          *shall—*

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

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

22          **“§ 3596. Training**

23               “(a) COVERED INDIVIDUAL DEFINED.—*In this section,*  
 24               *the term ‘covered individual’ means an individual who ob-*

1 tains access to a Federal information system because of the  
 2 status of the individual as—

3 “(1) an employee, contractor, awardee, volunteer,  
 4 or intern of an agency; or

5 “(2) an employee of a contractor or awardee of  
 6 an agency.

7 “(b) *BEST PRACTICES AND CONSISTENCY.*—The Direc-  
 8 tor of the Cybersecurity and Infrastructure Security Agen-  
 9 cy, in consultation with the Director, the National Cyber  
 10 Director, and the Director of the National Institute of  
 11 Standards and Technology, shall develop best practices to  
 12 support consistency across agencies in cybersecurity inci-  
 13 dent response training, including—

14 “(1) information to be collected and shared with  
 15 the Cybersecurity and Infrastructure Security Agency  
 16 pursuant to section 3594(a) and processes for sharing  
 17 such information; and

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

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

23 “(1) the internal process of the agency for report-  
 24 ing an incident; and

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

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

9           **“§ 3597. Analysis and report on Federal incidents**

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

11               “(1) *QUANTITATIVE AND QUALITATIVE ANAL-*  
 12               *YSES.*—The Director of the Cybersecurity and Infra-  
 13               structure Security Agency shall perform and, in co-  
 14               ordination with the Director and the National Cyber  
 15               Director, develop, continuous monitoring and quan-  
 16               titative and qualitative analyses of incidents at agen-  
 17               cies, including major incidents, including—

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

19                               “(i) attacker tactics, techniques, and  
 20                               procedures; and

21                               “(ii) system vulnerabilities, including  
 22                               zero days, unpatched systems, and informa-  
 23                               tion system misconfigurations;

24                       “(B) the scope and scale of incidents at  
 25                       agencies;

1           “(C) *common root causes of incidents across*  
2           *multiple agencies;*

3           “(D) *agency incident response, recovery,*  
4           *and remediation actions and the effectiveness of*  
5           *those actions, as applicable;*

6           “(E) *lessons learned and recommendations*  
7           *in responding to, recovering from, remediating,*  
8           *and mitigating future incidents; and*

9           “(F) *trends across multiple agencies to ad-*  
10          *dress intrusion detection and incident response*  
11          *capabilities using the metrics established under*  
12          *section 224(c) of the Cybersecurity Act of 2015 (6*  
13          *U.S.C. 1522(c)).*

14          “(2) *AUTOMATED ANALYSIS.—The analyses de-*  
15          *veloped under paragraph (1) shall, to the greatest ex-*  
16          *tent practicable, use machine readable data, automa-*  
17          *tion, and machine learning processes.*

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

19                 “(A) *IN GENERAL.—The Director of the Cy-*  
20                 *bersecurity and Infrastructure Security Agency*  
21                 *shall share on an ongoing basis the analyses and*  
22                 *underlying data required under this subsection*  
23                 *with agencies, the Director, and the National*  
24                 *Cyber Director to—*

1                   “(i) improve the understanding of cy-  
2                   bersecurity risk of agencies; and

3                   “(ii) support the cybersecurity im-  
4                   provement efforts of agencies.

5                   “(B) *FORMAT*.—In carrying out subpara-  
6                   graph (A), the Director of the Cybersecurity and  
7                   Infrastructure Security Agency shall share the  
8                   analyses—

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

11                  “(ii) to the greatest extent practicable,  
12                  in machine-readable formats in order to en-  
13                  able automated intake and use by agencies.

14                  “(C) *EXEMPTION*.—This subsection shall  
15                  not apply to incidents that occur exclusively on  
16                  national security systems.

17                  “(b) *ANNUAL REPORT ON FEDERAL INCIDENTS*.—Not  
18                  later than 2 years after the date of enactment of this section,  
19                  and not less frequently than annually thereafter, the Direc-  
20                  tor of the Cybersecurity and Infrastructure Security Agen-  
21                  cy, in consultation with the Director, the National Cyber  
22                  Director and the heads of other agencies, as appropriate,  
23                  shall submit to the appropriate reporting entities a report  
24                  that includes—

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

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

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

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

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

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

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

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

21           “(c) PUBLICATION.—

22                 “(1) IN GENERAL.—The Director of the Cyberse-  
23 curity and Infrastructure Security Agency shall make  
24 a version of each report submitted under subsection  
25 (b) publicly available on the website of the Cybersecu-



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

3            “(2) *EXEMPTION.—The publication requirement*  
4        *under paragraph (1) shall not apply to a portion of*  
5        *a report that contains content that should be protected*  
6        *in the interest of national security, as determined by*  
7        *the Director, the Director of the Cybersecurity and In-*  
8        *frastructure Security Agency, or the National Cyber*  
9        *Director.*

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

14          “(4) *REQUIREMENT FOR COMPILING INFORMA-*  
15        *TION.—*

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

22            “(B) *EXCEPTION.—The Director of the Cy-*  
23        *bersecurity and Infrastructure Security Agency*  
24        *may include information that enables a specific*

1           *incident of an agency to be identified in a pub-*  
 2           *licly available report—*

3                   “(i) *with the concurrence of the Direc-*  
 4                   *tor and the National Cyber Director;*

5                   “(ii) *in consultation with the impacted*  
 6                   *agency; and*

7                   “(iii) *in consultation with the inspec-*  
 8                   *tor general of the impacted agency.*

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

10                   “(1) *IN GENERAL.—The analysis required under*  
 11                   *subsection (a) and each report submitted under sub-*  
 12                   *section (b) shall use information provided by agencies*  
 13                   *under section 3594(a).*

14                   “(2) *NONCOMPLIANCE REPORTS.—During any*  
 15                   *year during which the head of an agency does not*  
 16                   *provide data for an incident to the Cybersecurity and*  
 17                   *Infrastructure Security Agency in accordance with*  
 18                   *section 3594(a), the head of the agency, in coordina-*  
 19                   *tion with the Director of the Cybersecurity and Infra-*  
 20                   *structure Security Agency and the Director, shall sub-*  
 21                   *mit to the appropriate reporting entities a report that*  
 22                   *includes the information described in subsection (b)*  
 23                   *with respect to the agency.*

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

1           “(1) *IN GENERAL.*—Notwithstanding any other  
2           *provision of this section, the Secretary of Defense, in*  
3           *consultation with the Director, the National Cyber*  
4           *Director, the Director of National Intelligence, and*  
5           *the Director of Cybersecurity and Infrastructure Se-*  
6           *curity shall annually submit a report that includes*  
7           *the information described in subsection (b) with re-*  
8           *spect to national security systems, to the extent that*  
9           *the submission is consistent with standards and*  
10          *guidelines for national security systems issued in ac-*  
11          *cordance with law and as directed by the President,*  
12          *to—*

13               “(A) *the majority and minority leaders of*  
14               *the Senate,*

15               “(B) *the Speaker and minority leader of the*  
16               *House of Representatives;*

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

19               “(D) *the Select Committee on Intelligence of*  
20               *the Senate;*

21               “(E) *the Committee on Armed Services of*  
22               *the Senate;*

23               “(F) *the Committee on Appropriations of*  
24               *the Senate;*

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

3                   “(H) *the Committee on Homeland Security*  
4                   *of the House of Representatives;*

5                   “(I) *the Permanent Select Committee on In-*  
6                   *telligence of the House of Representatives;*

7                   “(J) *the Committee on Armed Services of*  
8                   *the House of Representatives; and*

9                   “(K) *the Committee on Appropriations of*  
10                  *the House of Representatives.*

11                  “(2) *CLASSIFIED FORM.—A report required*  
12                  *under paragraph (1) may be submitted in a classified*  
13                  *form.*

14   **“§ 3598. Major incident definition**

15                  “(a) *IN GENERAL.—Not later than 1 year after the*  
16                  *later of the date of enactment of the Federal Information*  
17                  *Security Modernization Act of 2023 and the most recent*  
18                  *publication by the Director of guidance to agencies regard-*  
19                  *ing major incidents as of the date of enactment of the Fed-*  
20                  *eral Information Security Modernization Act of 2023, the*  
21                  *Director shall develop, in coordination with the National*  
22                  *Cyber Director, and promulgate guidance on the definition*  
23                  *of the term ‘major incident’ for the purposes of subchapter*  
24                  *II and this subchapter.*

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

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

7                       “(A) any incident the head of the agency  
 8 determines is likely to result in demonstrable  
 9 harm to—

10                               “(i) the national security interests, for-  
 11 eign relations, homeland security, or eco-  
 12 nomic security of the United States; or

13                               “(ii) the civil liberties, public con-  
 14 fidence, privacy, or public health and safety  
 15 of the people of the United States;

16                       “(B) any incident the head of the agency  
 17 determines likely to result in an inability or sub-  
 18 stantial disruption for the agency, a component  
 19 of the agency, or the Federal Government, to pro-  
 20 vide 1 or more critical services;

21                       “(C) any incident the head of the agency  
 22 determines substantially disrupts or substan-  
 23 tially degrades the operations of a high value  
 24 asset owned or operated by the agency;

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

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

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

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

16               “(B) is enabled by—

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

21                       “(ii) the related activities of a common  
 22                       threat actor;

23           “(3) stipulate that, in determining whether an  
 24          incident constitutes a major incident under the stand-  
 25          ards described in paragraph (1), the head of the agen-

1        *cy shall consult with the National Cyber Director;*  
2        *and*

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

7        *“(c) EVALUATION AND UPDATES.—Not later than 60*  
8        *days after the date on which the Director first promulgates*  
9        *the guidance required under subsection (a), and not less fre-*  
10       *quently than once during the first 90 days of each evenly*  
11       *numbered Congress thereafter, the Director shall provide to*  
12       *the Committee on Homeland Security and Governmental*  
13       *Affairs of the Senate and the Committees on Oversight and*  
14       *Accountability and Homeland Security of the House of*  
15       *Representatives a briefing that includes—*

16                *“(1) an evaluation of any necessary updates to*  
17        *the guidance;*

18                *“(2) an evaluation of any necessary updates to*  
19        *the definition of the term ‘major incident’ included in*  
20        *the guidance; and*

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

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

“3591. *Definitions.*

“3592. *Notification of breach.*

“3593. *Congressional and Executive Branch reports.*

“3594. *Government information sharing and incident response.*

“3595. *Responsibilities of contractors and awardees.*

“3596. *Training.*

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

“3598. *Major incident definition.*”.

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

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

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

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

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

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

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

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

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



1           “(B) require that any proposal for the use  
2 of amounts in the Fund includes, as appro-  
3 priate—

4                 “(i) a cybersecurity risk management  
5 plan; and

6                 “(ii) a supply chain risk assessment in  
7 accordance with section 1326 of title 41.”;  
8 and

9 (3) in subsection (c)—

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

13                (B) in paragraph (5)—

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

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

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

21                 “(C) a senior official from the Cybersecurity  
22 and Infrastructure Security Agency of the De-  
23 partment of Homeland Security, appointed by  
24 the Director.”; and

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

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

6                   (1) in section 11302—

7                   (A) in subsection (b), by striking “use, secu-  
8                   rity, and disposal of” and inserting “use, and  
9                   disposal of, and, in consultation with the Direc-  
10                  tor of the Cybersecurity and Infrastructure Secu-  
11                  rity Agency and the National Cyber Director,  
12                  promote and improve the security of,”; and

13                  (B) in subsection (h), by inserting “, in-  
14                  cluding cybersecurity performances,” after “the  
15                  performances”; and

16                  (2) in section 11303(b)(2)(B)—

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

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

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

22                           “(iii) whether the function should be  
23                           performed by a shared service offered by an-  
24                           other executive agency;”.

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

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

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

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

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

13 **SEC. 105. ACTIONS TO ENHANCE FEDERAL INCIDENT**  
14 **TRANSPARENCY.**

15       (a) *RESPONSIBILITIES OF THE CYBERSECURITY AND*  
16 *INFRASTRUCTURE SECURITY AGENCY.*—

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

21           (A) develop a plan for the development of  
22 the analysis required under section 3597(a) of  
23 title 44, United States Code, as added by this  
24 title, and the report required under subsection

25           (b) of that section that includes—

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

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

9                   (B) provide to the appropriate congressional  
 10                  committees a briefing on the plan developed  
 11                  under subparagraph (A).

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

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

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

22               (b) *RESPONSIBILITIES OF THE DIRECTOR OF THE OF-*  
 23               *FICE OF MANAGEMENT AND BUDGET.*—

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

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

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

8           (2) *INCIDENT DATA SHARING.*—

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

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

19                             (i) *enable the efficient development*  
20                             *of—*

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

1                   (II) *the report on Federal inci-*  
2                   *dents required under section 3597(b) of*  
3                   *title 44, United States Code, as added*  
4                   *by this title; and*  
5                   (ii) *include requirements for the time-*  
6                   *liness of data production.*

7                   (C) *AUTOMATION.—The Director, in coordi-*  
8                   *nation with the Director of the Cybersecurity*  
9                   *and Infrastructure Security Agency, shall pro-*  
10                  *mote, as feasible, the use of automation and ma-*  
11                  *chine-readable data for data sharing under sec-*  
12                  *tion 3594(a) of title 44, United States Code, as*  
13                  *added by this title.*

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

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

23                  (B) *EXISTING PROCESSES.—To the greatest*  
24                  *extent practicable, the guidance issued under*  
25                  *subparagraph (A) shall allow contractors and*

1            *awardees to use existing processes for notifying*  
 2            *agencies of incidents involving information of*  
 3            *the Federal Government.*

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

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

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

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

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

18    **SEC. 106. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**

19                    **UPDATES.**

20            *(a) IN GENERAL.—Not later than 1 year after the date*  
 21            *of enactment of this Act, the Director shall issue guidance*  
 22            *for agencies on—*

23            *(1) performing the ongoing and continuous agen-*  
 24            *cy system risk assessment required under section*

1       3554(a)(1)(A) of title 44, United States Code, as  
2       amended by this title; and

3               (2) establishing a process for securely providing  
4       the status of each remedial action for high value as-  
5       sets under section 3554(b)(7) of title 44, United States  
6       Code, as amended by this title, to the Director and the  
7       Director of the Cybersecurity and Infrastructure Se-  
8       curity Agency using automation and machine-read-  
9       able data, as practicable, which shall include—

10               (A) specific guidance for the use of automa-  
11       tion and machine-readable data; and

12               (B) templates for providing the status of the  
13       remedial action.

14       (b) *COORDINATION.*—The head of each agency shall co-  
15       ordinate with the inspector general of the agency, as appli-  
16       cable, to ensure consistent understanding of agency policies  
17       for the purpose of evaluations conducted by the inspector  
18       general.

19       **SEC. 107. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**  
20       **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

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

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



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

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

15                 *(1) the confidentiality or integrity of sensitive*  
16                 *information submitted by the reporting entity to the*  
17                 *agency pursuant to a statutory or regulatory require-*  
18                 *ment; or*

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

1 **SEC. 108. MOBILE SECURITY BRIEFINGS.**

2       (a) *IN GENERAL.*—Not later than 180 days after the  
3 date of enactment of this Act, the Director shall provide to  
4 the appropriate congressional committees—

5           (1) a briefing on the compliance of agencies with  
6 the No TikTok on Government Devices Act (44 U.S.C.  
7 3553 note; Public Law 117–328); and

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

13       (b) *ADDITIONAL BRIEFING.*—Not later than 1 year  
14 after the date of the briefing required under subsection  
15 (a)(1), the Director shall provide to the appropriate con-  
16 gressional committees—

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

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

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

3 (a) *GUIDANCE.*—Not later than 2 years after the date  
4 of enactment of this Act, the Director, in consultation with  
5 the National Cyber Director and the Director of the Cyber-  
6 security and Infrastructure Security Agency, shall update  
7 guidance to agencies regarding requirements for logging, log  
8 retention, log management, sharing of log data with other  
9 appropriate agencies, or any other logging activity deter-  
10 mined to be appropriate by the Director.

11 (b) *NATIONAL SECURITY SYSTEMS.*—The Secretary of  
12 Defense shall issue guidance that meets or exceeds the stand-  
13 ards required in guidance issued under subsection (a) for  
14 National Security Systems.

15 **SEC. 110. CISA AGENCY LIAISONS.**

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

23 (b) *QUALIFICATIONS.*—Each liaison assigned under  
24 subsection (a) shall have knowledge of—

25 (1) *cybersecurity threats facing agencies, includ-*  
26 *ing any specific threats to the assigned agency;*

1           (2) *risk assessments of agency systems; and*

2           (3) *other Federal cybersecurity initiatives.*

3       (c) *DUTIES.—The duties of each liaison assigned*  
4 *under subsection (a) shall include—*

5           (1) *providing, as requested, assistance and ad-*  
6 *vice to the agency Chief Information Security Officer;*

7           (2) *supporting, as requested, incident response*  
8 *coordination between the assigned agency and the Cy-*  
9 *bersecurity and Infrastructure Security Agency;*

10          (3) *becoming familiar with assigned agency sys-*  
11 *tems, processes, and procedures to better facilitate*  
12 *support to the agency; and*

13          (4) *other liaison duties to the assigned agency*  
14 *solely in furtherance of Federal cybersecurity or sup-*  
15 *port to the assigned agency as a Sector Risk Manage-*  
16 *ment Agency, as assigned by the Director of the Cy-*  
17 *bersecurity and Infrastructure Security Agency in*  
18 *consultation with the head of the assigned agency.*

19       (d) *LIMITATION.—A liaison assigned under subsection*  
20 *(a) shall not be a contractor.*

21       (e) *MULTIPLE ASSIGNMENTS.—One individual liaison*  
22 *may be assigned to multiple agency Chief Information Se-*  
23 *curity Officers under subsection (a).*

24       (f) *COORDINATION OF ACTIVITIES.—The Director of*  
25 *the Cybersecurity and Infrastructure Security Agency shall*

1 *consult with the Director on the execution of the duties of*  
 2 *the Cybersecurity and Infrastructure Security Agency liai-*  
 3 *sons to ensure that there is no inappropriate duplication*  
 4 *of activities among—*

5           (1) *Federal cybersecurity support to agencies of*  
 6 *the Office of Management and Budget; and*

7           (2) *the Cybersecurity and Infrastructure Secu-*  
 8 *rity Agency liaison.*

9           (g) *RULE OF CONSTRUCTION.—Nothing in this section*  
 10 *shall be construed impact the ability of the Director to sup-*  
 11 *port agency implementation of Federal cybersecurity re-*  
 12 *quirements pursuant to subchapter II of chapter 35 of title*  
 13 *44, United States Code, as amended by this title.*

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

15           (a) *IN GENERAL.—Subchapter II of chapter 35 of title*  
 16 *44, United States Code, is amended by adding at the end*  
 17 *the following:*

18 **“§ 3559A. Federal penetration testing**

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

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

1           “(2) provides policies governing the development  
2 of—

3                   “(A) rules of engagement for using penetra-  
4 tion testing; and

5                   “(B) procedures to use the results of pene-  
6 tration testing to improve the cybersecurity and  
7 risk management of the agency;

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

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

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

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

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

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

25           (b) *EXISTING GUIDANCE.—*

1           (1) *IN GENERAL.*—*Compliance with guidance*  
 2           *issued by the Director relating to penetration testing*  
 3           *before the date of enactment of this Act shall be*  
 4           *deemed to be compliance with section 3559A of title*  
 5           *44, United States Code, as added by this title.*

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

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

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

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

1           “(9) performing penetration testing that may le-  
 2           verage manual expert analysis to identify threats and  
 3           vulnerabilities within information systems—

4                   “(A) without consent or authorization from  
 5           agencies; and

6                   “(B) with prior notification to the head of  
 7           the agency;”.

8   **SEC. 112. VULNERABILITY DISCLOSURE POLICIES.**

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

12   **“§ 3559B. Federal vulnerability disclosure policies**

13           “(a) *PURPOSE; SENSE OF CONGRESS.*—

14                   “(1) *PURPOSE.*—The purpose of Federal vulner-  
 15           ability disclosure policies is to create a mechanism to  
 16           enable the public to inform agencies of vulnerabilities  
 17           in Federal information systems.

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

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



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

3           “(2) *INTERNET OF THINGS*.—The term ‘internet  
4           of things’ has the meaning given the term in Special  
5           Publication 800–213 of the National Institute of  
6           Standards and Technology, entitled ‘IoT Device Cy-  
7           bersecurity Guidance for the Federal Government: Es-  
8           tablishing IoT Device Cybersecurity Requirements’, or  
9           any successor document.

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

14          “(4) *SUBMITTER*.—The term ‘submitter’ means  
15          an individual that submits a vulnerability disclosure  
16          report pursuant to the vulnerability disclosure process  
17          of an agency.

18          “(5) *VULNERABILITY DISCLOSURE REPORT*.—The  
19          term ‘vulnerability disclosure report’ means a disclo-  
20          sure of a security vulnerability made to an agency by  
21          a submitter.

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

24                 “(1) use of the information system security  
25                 vulnerabilities disclosure process guidelines estab-

1 *lished under section 4(a)(1) of the IoT Cybersecurity*  
2 *Improvement Act of 2020 (15 U.S.C. 278g–3b(a)(1));*

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

6 *“(A) represents a good faith effort to iden-*  
7 *tify and report security vulnerabilities in infor-*  
8 *mation systems; or*

9 *“(B) otherwise represents a good faith effort*  
10 *to follow the vulnerability disclosure policy of the*  
11 *agency developed under subsection (f)(2);*

12 *“(3) direction on sharing relevant information*  
13 *in a consistent, automated, and machine readable*  
14 *manner with the Director of the Cybersecurity and*  
15 *Infrastructure Security Agency;*

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

20 *“(5) requirements for providing information to*  
21 *the submitter of a vulnerability disclosure report on*  
22 *the resolution of the vulnerability disclosure report;*

23 *“(6) a stipulation that the mere identification by*  
24 *a submitter of a security vulnerability, without a sig-*

1        *nificant compromise of confidentiality, integrity, or*  
2        *availability, does not constitute a major incident; and*

3                *“(7) the applicability of the guidance to Internet*  
4        *of things devices owned or controlled by an agency.*

5        *“(d) CONSULTATION.—In developing the guidance re-*  
6        *quired under subsection (c)(3), the Director shall consult*  
7        *with the Director of the Cybersecurity and Infrastructure*  
8        *Security Agency.*

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

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

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

16                *“(3) upon a request by an agency, assist the*  
17        *agency in the disclosure to vendors of newly identified*  
18        *security vulnerabilities in vendor products and serv-*  
19        *ices; and*

20                *“(4) as appropriate, implement the requirements*  
21        *of this section, in accordance with the authority*  
22        *under section 3553(b)(8), as a shared service available*  
23        *to agencies.*

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

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

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

8                       “(B) *the component of the agency that is re-*  
 9                       *sponsible for the internet accessible services of-*  
 10                      *fered at the domain.*

11           “(2) *VULNERABILITY DISCLOSURE POLICY.*—*The*  
 12           *head of each agency shall develop and make publicly*  
 13           *available a vulnerability disclosure policy for the*  
 14           *agency, which shall—*

15                      “(A) *describe—*

16                               “(i) *the scope of the systems of the*  
 17                               *agency included in the vulnerability disclo-*  
 18                               *sure policy, including for Internet of things*  
 19                               *devices owned or controlled by the agency;*

20                              “(ii) *the type of information system*  
 21                              *testing that is authorized by the agency;*

22                              “(iii) *the type of information system*  
 23                              *testing that is not authorized by the agency;*

24                              “(iv) *the disclosure policy for a con-*  
 25                              *tractor; and*

1                   “(v) the disclosure policy of the agency  
2                   for sensitive information;

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

5                   “(i) how the submitter should submit  
6                   the vulnerability disclosure report; and

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

11                  “(C) include any other relevant informa-  
12                  tion; and

13                  “(D) be mature in scope and cover every  
14                  internet accessible information system used or  
15                  operated by that agency or on behalf of that  
16                  agency.

17                  “(3) IDENTIFIED SECURITY VULNERABILITIES.—  
18                  The head of each agency shall—

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

21                  “(B) commensurate with the risk posed by  
22                  the security vulnerability, address such security  
23                  vulnerability using the security vulnerability  
24                  management process of the agency; and

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

4           “(g) EXEMPTIONS.—

5           “(1) IN GENERAL.—The Director and the head of  
 6           each agency shall carry out this section in a manner  
 7           consistent with the protection of national security in-  
 8           formation.

9           “(2) LIMITATION.—The Director and the head of  
 10          each agency may not publish under subsection (f)(1)  
 11          or include in a vulnerability disclosure policy under  
 12          subsection (f)(2) host names, services, information  
 13          systems, or other information that the Director or the  
 14          head of an agency, in coordination with the Director  
 15          and other appropriate heads of agencies, determines  
 16          would—

17               “(A) disrupt a law enforcement investiga-  
 18               tion;

19               “(B) endanger national security or intel-  
 20               ligence activities; or

21               “(C) impede national defense activities or  
 22               military operations.

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

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

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

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

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

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

“3559B. *Federal vulnerability disclosure policies.*”.

17       (c) *CONFORMING UPDATE AND REPEAL.—*

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

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

4                     *(A) by striking section 6 (15 U.S.C. 278g–*  
 5                     *3d); and*

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

8   **SEC. 113. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

9           *(a) BRIEFINGS.—Not later than 1 year after the date*  
 10          *of enactment of this Act, the Director shall provide to the*  
 11          *Committee on Homeland Security and Governmental Af-*  
 12          *fairs of the Senate and the Committees on Oversight and*  
 13          *Accountability and Homeland Security of the House of*  
 14          *Representatives a briefing on progress in increasing the in-*  
 15          *ternal defenses of agency systems, including—*

16                    *(1) shifting away from trusted networks to im-*  
 17                    *plement security controls based on a presumption of*  
 18                    *compromise, including through the transition to zero*  
 19                    *trust architecture;*

20                    *(2) implementing principles of least privilege in*  
 21                    *administering information security programs;*

22                    *(3) limiting the ability of entities that cause in-*  
 23                    *cidents to move laterally through or between agency*  
 24                    *systems;*

25                    *(4) identifying incidents quickly;*



1           (5) *isolating and removing unauthorized entities*  
2           *from agency systems as quickly as practicable, ac-*  
3           *counting for intelligence or law enforcement purposes;*  
4           *and*

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

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

15               (1) *a description of steps agencies have com-*  
16               *pleted, including progress toward achieving any re-*  
17               *quirements issued by the Director, including the*  
18               *adoption of any models or reference architecture;*

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

22               (3) *a schedule to implement any planned activi-*  
23               *ties.*

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

4       (d) *NATIONAL SECURITY SYSTEMS.*—

5           (1) *BRIEFING.*—Not later than 1 year after the  
6 date of enactment of this Act, the Secretary of Defense  
7 shall provide to the Committee on Homeland Security  
8 and Governmental Affairs of the Senate, the Com-  
9 mittee on Oversight and Accountability of the House  
10 of Representatives, the Committee on Armed Services  
11 of the Senate, the Committee on Armed Services of the  
12 House of Representatives, the Select Committee on In-  
13 telligence of the Senate, and the Permanent Select  
14 Committee on Intelligence of the House of Representa-  
15 tives a briefing on the implementation of zero trust  
16 architecture with respect to national security systems.

17          (2) *PROGRESS REPORT.*—Not later than the date  
18 on which each update is required to be submitted  
19 under subsection (b), the Secretary of Defense shall  
20 submit to the congressional committees described in  
21 paragraph (1) a progress report on the implementa-  
22 tion of zero trust architecture with respect to national  
23 security systems.

1 **SEC. 114. AUTOMATION AND ARTIFICIAL INTELLIGENCE.**

2 (a) *DEFINITION.*—In this section, the term “informa-  
3 tion system” has the meaning given the term in section  
4 3502 of title 44, United States Code.

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

6 (1) *IN GENERAL.*—As appropriate, the Director  
7 shall issue guidance on the use of artificial intel-  
8 ligence by agencies to improve the cybersecurity of in-  
9 formation systems.

10 (2) *CONSIDERATIONS.*—The Director and head of  
11 each agency shall consider the use and capabilities of  
12 artificial intelligence systems wherever automation is  
13 used in furtherance of the cybersecurity of informa-  
14 tion systems.

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

22 (c) *COMPTROLLER GENERAL REPORTS.*—

23 (1) *IN GENERAL.*—Not later than 2 years after  
24 the date of enactment of this Act, the Comptroller  
25 General of the United States shall submit to the ap-  
26 propriate congressional committees a report on the

1 *risks to the privacy of individuals and the cybersecu-*  
2 *urity of information systems associated with the use by*  
3 *Federal agencies of artificial intelligence systems or*  
4 *capabilities.*

5 (2) *STUDY.*—*Not later than 2 years after the*  
6 *date of enactment of this Act, the Comptroller General*  
7 *of the United States shall perform a study, and sub-*  
8 *mit to the Committees on Homeland Security and*  
9 *Governmental Affairs and Commerce, Science, and*  
10 *Transportation of the Senate and the Committees on*  
11 *Oversight and Accountability, Homeland Security,*  
12 *and Science, Space, and Technology of the House of*  
13 *Representatives a report, on the use of automation,*  
14 *including artificial intelligence, and machine-read-*  
15 *able data across the Federal Government for cyberse-*  
16 *curity purposes, including the automated updating of*  
17 *cybersecurity tools, sensors, or processes employed by*  
18 *agencies under paragraphs (1), (5)(C), and (8)(B) of*  
19 *section 3554(b) of title 44, United States Code, as*  
20 *amended by this title.*

21 **SEC. 115. EXTENSION OF CHIEF DATA OFFICER COUNCIL.**

22 *Section 3520A(e)(2) of title 44, United States Code,*  
23 *is amended by striking “upon the expiration of the 2-year*  
24 *period that begins on the date the Comptroller General sub-*

1 mits the report under paragraph (1) to Congress” and in-  
 2 serting “December 31, 2031”.

3 **SEC. 116. COUNCIL OF THE INSPECTORS GENERAL ON IN-**  
 4 **TEGRITY AND EFFICIENCY DASHBOARD.**

5 (a) *DASHBOARD REQUIRED.*—Section 424(e) of title 5,  
 6 United States Code, is amended—

7 (1) in paragraph (2)—

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

10 (B) by redesignating subparagraph (B) as  
 11 subparagraph (C);

12 (C) by inserting after subparagraph (A) the  
 13 following:

14 “(B) that shall include a dashboard of open  
 15 information security recommendations identified  
 16 in the independent evaluations required by sec-  
 17 tion 3555(a) of title 44; and”; and

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

19 “(5) *RULE OF CONSTRUCTION.*—Nothing in this  
 20 subsection shall be construed to require the publica-  
 21 tion of information that is exempted from disclosure  
 22 under section 552 of this title.”.

1 **SEC. 117. SECURITY OPERATIONS CENTER SHARED SERV-**  
2 **ICE.**

3 (a) *BRIEFING.*—Not later than 180 days after the date  
4 of enactment of this Act, the Director of the Cybersecurity  
5 and Infrastructure Security Agency shall provide to the  
6 Committee on Homeland Security and Governmental Af-  
7 fairs of the Senate and the Committee on Homeland Secu-  
8 rity and the Committee on Oversight and Accountability  
9 of the House of Representatives a briefing on—

10 (1) *existing security operations center shared*  
11 *services;*

12 (2) *the capability for such shared service to offer*  
13 *centralized and simultaneous support to multiple*  
14 *agencies;*

15 (3) *the capability for such shared service to inte-*  
16 *grate with or support agency threat hunting activities*  
17 *authorized under section 3553 of title 44, United*  
18 *States Code, as amended by this title;*

19 (4) *the capability for such shared service to inte-*  
20 *grate with or support Federal vulnerability manage-*  
21 *ment activities; and*

22 (5) *future plans for expansion and maturation*  
23 *of such shared service.*

24 (b) *GAO REPORT.*—Not less than 540 days after the  
25 date of enactment of this Act, the Comptroller General of  
26 the United States shall submit to the appropriate congres-

1 sional committees a report on Federal cybersecurity secu-  
 2 rity operations centers that—

3 (1) identifies Federal agency best practices for ef-  
 4 ficiency and effectiveness;

5 (2) identifies non-Federal best practices used by  
 6 large entity operations centers and entities providing  
 7 operation centers as a service; and

8 (3) includes recommendations for the Cybersecu-  
 9 rity and Infrastructure Security Agency and any  
 10 other relevant agency to improve the efficiency and ef-  
 11 fectiveness of security operations centers shared serv-  
 12 ice offerings.

13 **SEC. 118. 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 title, 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 a single sign-on trusted*  
18                    *identity platform for individuals accessing each*  
19                    *public website of the agency that requires user*  
20                    *authentication, as developed by the Adminis-*  
21                    *trator of General Services in collaboration with*  
22                    *the Secretary; and*

23                    “(E) *implement identity management con-*  
24                    *sistent with section 504 of the Cybersecurity En-*



1        *hancement Act of 2014 (15 U.S.C. 7464), includ-*  
2        *ing multi-factor authentication, for—*

3                *“(i) remote access to an information*  
4                *system; and*

5                *“(ii) each user account with elevated*  
6                *privileges on a information system.*

7        *“(2) PROHIBITION.—*

8                *“(A) DEFINITION.—In this paragraph, the*  
9                *term ‘Internet of things’ has the meaning given*  
10               *the term in section 3559B.*

11               *“(B) PROHIBITION.—Consistent with poli-*  
12               *cies, standards, guidelines, and directives on in-*  
13               *formation security under this subchapter, and*  
14               *except as provided under paragraph (3), the*  
15               *head of an agency may not procure, obtain,*  
16               *renew a contract to procure or obtain in any*  
17               *amount, notwithstanding section 1905 of title 41*  
18               *or use an Internet of things device if the Chief*  
19               *Information Officer of the agency determines*  
20               *during a review required under section*  
21               *11319(b)(1)(C) of title 40 of a contract for an*  
22               *Internet of things device that the use of the de-*  
23               *vice prevents compliance with the standards and*  
24               *guidelines developed under section 4 of the IoT*

1           *Cybersecurity Improvement Act (15 U.S.C.*  
2           *278g–3b) with respect to the device.*

3           “(3) *EXCEPTION.—The requirements under*  
4           *paragraph (1) shall not apply to an information sys-*  
5           *tem for which—*

6                     “(A) *the head of the agency, without delega-*  
7                     *tion, has certified to the Director with particu-*  
8                     *larity that—*

9                             “(i) *operational requirements articu-*  
10                            *lated in the certification and related to the*  
11                            *information system would make it exces-*  
12                            *sively burdensome to implement the cyberse-*  
13                            *curity requirement;*

14                           “(ii) *the cybersecurity requirement is*  
15                            *not necessary to secure the information sys-*  
16                            *tem or agency information stored on or*  
17                            *transiting it; and*

18                           “(iii) *the agency has taken all nec-*  
19                            *essary steps to secure the information sys-*  
20                            *tem and agency information stored on or*  
21                            *transiting it; and*

22                           “(B) *the head of the agency has submitted*  
23                            *the certification described in subparagraph (A)*  
24                            *to the appropriate congressional committees and*  
25                            *the authorizing 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*  
 7                   *(3)(A).*

8                   “(B) *RENEWAL.*—*Upon the expiration of a*  
 9                   *certification of an agency under paragraph (3),*  
 10                   *the head of the agency may submit an additional*  
 11                   *certification in accordance with that paragraph.*

12           “(5) *RULES OF CONSTRUCTION.*—*Nothing in this*  
 13           *subsection shall be construed—*

14                   “(A) *to alter the authority of the Secretary,*  
 15                   *the Director, or the Director of the National In-*  
 16                   *stitute of Standards and Technology in imple-*  
 17                   *menting subchapter II of this title;*

18                   “(B) *to affect the standards or process of the*  
 19                   *National Institute of Standards and Technology;*

20                   “(C) *to affect the requirement under section*  
 21                   *3553(a)(4); or*

22                   “(D) *to discourage continued improvements*  
 23                   *and advancements in the technology, standards,*  
 24                   *policies, and guidelines used to promote Federal*  
 25                   *information security.*

1 “(g) *EXCEPTION.*—

2 “(1) *REQUIREMENTS.*—*The requirements under*  
3 *subsection (f)(1) shall not apply to—*

4 “(A) *the Department of Defense;*

5 “(B) *a national security system; or*

6 “(C) *an element of the intelligence commu-*  
7 *nity.*

8 “(2) *PROHIBITION.*—*The prohibition under sub-*  
9 *section (f)(2) shall not apply to—*

10 “(A) *Internet of things devices that are or*  
11 *comprise a national security system;*

12 “(B) *national security systems; or*

13 “(C) *a procured Internet of things device*  
14 *described in subsection (f)(2)(B) that the Chief*  
15 *Information Officer of an agency determines is—*

16 “(i) *necessary for research purposes; or*

17 “(ii) *secured using alternative and ef-*  
18 *fective methods appropriate to the function*  
19 *of the Internet of things device.”.*

20 (b) *REPORT ON EXEMPTIONS.*—*Section 3554(c)(1) of*  
21 *title 44, United States Code, as amended by this title, is*  
22 *further amended—*

23 (1) *in subparagraph (B), by striking “and” at*  
24 *the end;*

1           (2) *in subparagraph (C), by striking the period*  
 2           *at the end and inserting “; and”; and*

3           (3) *by adding at the end the following:*

4                   “(D) *with respect to any exemption from*  
 5                   *the requirements of subsection (f)(3) that is effec-*  
 6                   *tive on the date of submission of the report, in-*  
 7                   *cludes the number of information systems that*  
 8                   *have received an exemption from those require-*  
 9                   *ments.”.*

10          (c) *DURATION OF CERTIFICATION EFFECTIVE DATE.—*  
 11          *Paragraph (3) of section 3554(f) of title 44, United States*  
 12          *Code, as added by this title, shall take effect on the date*  
 13          *that is 1 year after the date of enactment of this Act.*

14          (d) *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. 119. 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 the enactment*  
 4 *of this Act may serve as the Federal Chief Information Se-*  
 5 *curity Officer under section 3617 of title 44, United States*  
 6 *Code, as added by this title, beginning on the date of enact-*  
 7 *ment of this Act, without need for a further or additional*  
 8 *appointment 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:*

“Sec. 3617. Federal chief information security officer”.

12 **SEC. 120. RENAMING OFFICE OF THE FEDERAL CHIEF IN-**  
 13 **FORMATION 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*.—Section  
 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 “OF-*  
 10                   *FICE OF THE FEDERAL CHIEF INFORMATION*  
 11                   *OFFICER”;*

12                   (2) *in subsection (a), by striking “Office of Elec-*  
 13                   *tronic Government” and inserting “Office of the Fed-*  
 14                   *eral Chief Information Officer”;*

15                   (3) *in subsection (b), by striking “an Adminis-*  
 16                   *trator” and inserting “a Federal Chief Information*  
 17                   *Officer”;*

18                   (4) *in subsection (c), in the matter preceding*  
 19                   *paragraph (1), by striking “The Administrator” and*  
 20                   *inserting “The Federal Chief Information Officer”;*

21                   (5) *in subsection (d), in the matter preceding*  
 22                   *paragraph (1), by striking “The Administrator” and*  
 23                   *inserting “The Federal Chief Information Officer”;*

(6) in subsection (e), in the matter preceding paragraph (1), by striking “The Administrator” and inserting “The Federal Chief Information Officer”;

(7) in subsection (f)—

(A) in the matter preceding paragraph (1), by striking “the Administrator” and inserting “the Federal Chief Information Officer”;

(B) in paragraph (16), by striking “the Office of Electronic Government” and inserting “the Office of the Federal Chief Information Officer”; and

(C) in paragraph (17), by striking “E-Government” and inserting “annual”; and

(8) in subsection (g), by striking “the Office of Electronic Government” and inserting “the Office of the Federal Chief Information Officer”.

(c) CHIEF INFORMATION OFFICERS COUNCIL.—Section 3603 of title 44, United States Code, is amended—

(1) in subsection (b)(2), by striking “The Administrator of the Office of Electronic Government” and inserting “The Federal Chief Information Officer”;

(2) in subsection (c)(1), by striking “The Administrator of the Office of Electronic Government” and inserting “The Federal Chief Information Officer”; and

1           (3) in subsection (f)—

2                   (A) in paragraph (3), by striking “the Ad-  
3                   ministrators” and inserting “the Federal Chief  
4                   Information Officer”; and

5                   (B) in paragraph (5), by striking “the Ad-  
6                   ministrators” and inserting “the Federal Chief  
7                   Information Officer”.

8           (d) *E-GOVERNMENT FUND*.—Section 3604 of title 44,  
9   *United States Code*, is amended—

10           (1) in subsection (a)(2), by striking “the Admin-  
11           istrator of the Office of Electronic Government” and  
12           inserting “the Federal Chief Information Officer”;

13           (2) in subsection (b), by striking “Adminis-  
14           trators” each place it appears and inserting “Federal  
15           Chief Information Officer”; and

16           (3) in subsection (c), in the matter preceding  
17           paragraph (1), by striking “the Administrator” and  
18           inserting “the Federal Chief Information Officer”.

19           (e) *PROGRAM TO ENCOURAGE INNOVATIVE SOLUTIONS*  
20   *TO ENHANCE ELECTRONIC GOVERNMENT SERVICES AND*  
21   *PROCESSES*.—Section 3605 of title 44, *United States Code*,  
22   is amended—

23           (1) in subsection (a), by striking “The Adminis-  
24           trator” and inserting “The Federal Chief Information  
25           Officer”;

(2) in subsection (b), by striking “, the Administrator,” and inserting “, the Federal Chief Information Officer,”; and

(3) in subsection (c)—

(A) in paragraph (1)—

(i) by striking “The Administrator” and inserting “The Federal Chief Information Officer”; and

(ii) by striking “proposals submitted to the Administrator” and inserting “proposals submitted to the Federal Chief Information Officer”;

(B) in paragraph (2)(B), by striking “the Administrator” and inserting “the Federal Chief Information Officer”; and

(C) in paragraph (4), by striking “the Administrator” and inserting “the Federal Chief Information Officer”.

(f) *E-GOVERNMENT REPORT*.—Section 3606 of title 44, United States Code, is amended—

(1) in the section heading by striking “**E-Government**” and inserting “**Annual**”;

(2) in subsection (a), by striking “E-Government” 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 the enactment of this Act, may continue*  
7 *to serve as the Federal Chief Information Officer com-*  
8 *mencing as of that date, without need for a further or addi-*  
9 *tional 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.*”; and

15           (2) *in the item relating to section 3606, by strik-*  
16 *ing “E–Government” and inserting “Annual”.*

17          (i) *REFERENCES.*—

18           (1) *ADMINISTRATOR.*—*Any reference to the Ad-*  
19 *ministrator of the Office of Electronic Government in*  
20 *any law, regulation, map, document, record, or other*  
21 *paper of the United States shall be deemed to be a ref-*  
22 *erence to the Federal Chief Information Officer.*

23           (2) *OFFICE OF ELECTRONIC GOVERNMENT.*—*Any*  
24 *reference to the Office of Electronic Government in*  
25 *any law, regulation, map, document, record, or other*

1        *paper of the United States shall be deemed to be a ref-*  
 2        *erence to the Office of the Federal Chief Information*  
 3        *Officer.*

4    **SEC. 121. RULES OF CONSTRUCTION.**

5        (a) *AGENCY ACTIONS.*—*Nothing in this title, or an*  
 6        *amendment made by this title, shall be construed to author-*  
 7        *ize the head of an agency to take an action that is not au-*  
 8        *thorized by this title, an amendment made by this title, or*  
 9        *existing law.*

10       (b) *PROTECTION OF RIGHTS.*—*Nothing in this title, or*  
 11       *an amendment made by this title, shall be construed to per-*  
 12       *mit the violation of the rights of any individual protected*  
 13       *by the Constitution of the United States, including through*  
 14       *censorship of speech protected by the Constitution of the*  
 15       *United States or unauthorized surveillance.*

16       (c) *PROTECTION OF PRIVACY.*—*Nothing in this title,*  
 17       *or an amendment made by this title, shall be construed to—*

18                (1) *impinge on the privacy rights of individuals;*

19        *or*

20                (2) *allow the unauthorized access, sharing, or use*  
 21        *of personal data.*

1 **TITLE II—RURAL HOSPITAL CY-**  
 2 **BERSECURITY            ENHANCE-**  
 3 **MENT ACT**

4 **SEC. 201. SHORT TITLE.**

5        *This title may be cited as the “Rural Hospital Cyber-*  
 6 *security Enhancement Act”.*

7 **SEC. 202. DEFINITIONS.**

8        *In this title:*

9            (1) *AGENCY.—The term “agency” has the mean-*  
 10 *ing given the term in section 551 of title 5, United*  
 11 *States Code.*

12            (2) *APPROPRIATE COMMITTEES OF CONGRESS.—*  
 13 *The term “appropriate committees of Congress”*  
 14 *means—*

15                    (A) *the Committee on Homeland Security*  
 16 *and Governmental Affairs of the Senate; and*

17                    (B) *the Committee on Homeland Security of*  
 18 *the House of Representatives.*

19            (3) *DIRECTOR.—The term “Director” means the*  
 20 *Director of the Cybersecurity and Infrastructure Se-*  
 21 *curity Agency.*

22            (4) *GEOGRAPHIC DIVISION.—The term “geo-*  
 23 *graphic division” means a geographic division that is*  
 24 *among the 9 geographic divisions determined by the*  
 25 *Bureau of the Census.*

1           (5) *RURAL HOSPITAL*.—The term “rural hos-  
2           pital” means a healthcare facility that—

3                   (A) is located in a non-urbanized area, as  
4                   determined by the Bureau of the Census; and

5                   (B) provides inpatient and outpatient  
6                   healthcare services, including primary care,  
7                   emergency care, and diagnostic services.

8           (6) *SECRETARY*.—The term “Secretary” means  
9           the Secretary of Homeland Security.

10 **SEC. 203. RURAL HOSPITAL CYBERSECURITY WORKFORCE**  
11 **DEVELOPMENT STRATEGY.**

12           (a) *IN GENERAL*.—Not later than 1 year after the date  
13 of enactment of this Act, the Secretary, acting through the  
14 Director, shall develop and transmit to the appropriate  
15 committees of Congress a comprehensive rural hospital cy-  
16 bersecurity workforce development strategy to address the  
17 growing need for skilled cybersecurity professionals in rural  
18 hospitals.

19           (b) *CONSULTATION*.—

20                   (1) *AGENCIES*.—In carrying out subsection (a),  
21 the Secretary and Director may consult with the Sec-  
22 retary of Health and Human Services, the Secretary  
23 of Education, the Secretary of Labor, and any other  
24 appropriate head of an agency.



1           (2) *PROVIDERS.*—*In carrying out subsection (a),*  
2           *the Secretary shall consult with not less than 2 rep-*  
3           *resentatives of rural healthcare providers from each*  
4           *geographic division in the United States.*

5           (c) *CONSIDERATIONS.*—*The rural hospital cybersecu-*  
6           *rity workforce development strategy developed under sub-*  
7           *section (a) shall, at a minimum, consider the following com-*  
8           *ponents:*

9           (1) *Partnerships between rural hospitals, non-*  
10           *rural healthcare systems, educational institutions,*  
11           *private sector entities, and nonprofit organizations to*  
12           *develop, promote, and expand the rural hospital cy-*  
13           *bersecurity workforce, including through education*  
14           *and training programs tailored to the needs of rural*  
15           *hospitals.*

16           (2) *The development of a cybersecurity cur-*  
17           *riculum and teaching resources that focus on teaching*  
18           *technical skills and abilities related to cybersecurity*  
19           *in rural hospitals for use in community colleges, vo-*  
20           *catiional schools, and other educational institutions lo-*  
21           *cated in rural areas.*

22           (3) *Identification of—*

23           (A) *cybersecurity workforce challenges that*  
24           *are specific to rural hospitals, as well as chal-*

1           *lenges that are relative to hospitals generally;*  
2           *and*

3                   *(B) common practices to mitigate both sets*  
4           *of challenges described in subparagraph (A).*

5           *(4) Recommendations for legislation, rule-*  
6           *making, or guidance to implement the components of*  
7           *the rural hospital cybersecurity workforce develop-*  
8           *ment strategy.*

9           *(d) ANNUAL BRIEFING.—Not later than 60 days after*  
10   *the date on which the first full fiscal year ends following*  
11   *the date on which the Secretary transmits the rural hospital*  
12   *cybersecurity workforce development strategy developed*  
13   *under subsection (a), and not later than 60 days after the*  
14   *date on which each fiscal year thereafter ends, the Secretary*  
15   *shall provide a briefing to the appropriate committees of*  
16   *Congress that includes, at a minimum, information relat-*  
17   *ing to—*

18                   *(1) updates to the rural hospital cybersecurity*  
19           *workforce development strategy, as appropriate;*

20                   *(2) any programs or initiatives established pur-*  
21           *suant to the rural hospital cybersecurity workforce de-*  
22           *velopment strategy, as well as the number of individ-*  
23           *uals trained or educated through such programs or*  
24           *initiatives;*

1           (3) *additional recommendations for legislation,*  
2           *rulemaking, or guidance to implement the components*  
3           *of the rural hospital cybersecurity workforce develop-*  
4           *ment strategy; and*

5           (4) *the effectiveness of the rural hospital cyberse-*  
6           *curity workforce development strategy in addressing*  
7           *the need for skilled cybersecurity professionals in*  
8           *rural hospitals.*

9   **SEC. 204. INSTRUCTIONAL MATERIALS FOR RURAL HOS-**  
10           **PITALS.**

11           (a) *IN GENERAL.*—*Not later than 1 year after the date*  
12           *of enactment of this Act, the Director shall make available*  
13           *instructional materials for rural hospitals that can be used*  
14           *to train staff on fundamental cybersecurity efforts.*

15           (b) *DUTIES.*—*In carrying out subsection (a), the Di-*  
16           *rector shall—*

17                   (1) *consult with appropriate heads of agencies,*  
18                   *experts in cybersecurity education, and rural*  
19                   *healthcare experts;*

20                   (2) *identify existing cybersecurity instructional*  
21                   *materials that can be adapted for use in rural hos-*  
22                   *pitals and create new materials as needed; and*

23                   (3) *conduct an awareness campaign to promote*  
24                   *the materials available to rural hospitals developed*  
25                   *under subsection (a).*

1 **SEC. 205. NO ADDITIONAL FUNDS.**

2       *No additional funds are authorized to be appropriated*

3 *for the purpose of carrying out this title.*



Calendar No. 674

118<sup>TH</sup> CONGRESS  
2<sup>D</sup> Session

**S. 2251**

[Report No. 118-271]

**A BILL**

To improve the cybersecurity of the Federal  
Government, and for other purposes.

DECEMBER 9, 2024

Reported with an amendment