

**AMENDMENT TO RULES COMMITTEE PRINT**  
**118-36**  
**OFFERED BY MS. MACE OF SOUTH CAROLINA**

At the end of subtitle C of title XVII, insert the following new section:

1 **SEC. 17\_\_\_.** **FEDERAL INFORMATION SECURITY MOD-**  
2 **ERNIZATION.**

3 (a) AMENDMENTS TO TITLE 44.—

4 (1) SUBCHAPTER I AMENDMENTS.—Subchapter  
5 I of chapter 35 of title 44, United States Code, is  
6 amended—

7 (A) in section 3504—

8 (i) in subsection (a)(1)(B)—

9 (I) by striking clause (v) and in-  
10 sserting the following:

11 “(v) privacy, confidentiality, disclosure,  
12 and sharing of information;”;

13 (II) by redesignating clause (vi)  
14 as clause (vii); and

15 (III) by inserting after clause (v)  
16 the following:

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

4                   (ii) in subsection (g)—

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

7                   (II) by striking paragraph (1)  
8                   and inserting the following:

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

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

18                  (B) in section 3505—

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

21                  (ii) in paragraph (2) of the second  
22                  subsection designated as subsection (c), by  
23                  inserting “an identification of internet ac-  
24                  cessible information systems and” after

1 “an inventory under this subsection shall  
2 include”;

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

5 (I) in subparagraph (B)—

6 (aa) by inserting “the Direc-  
7 tor of the Cybersecurity and In-  
8 frastructure Security Agency, the  
9 National Cyber Director, and”  
10 before “the Comptroller Gen-  
11 eral”; and

12 (bb) by striking “and” at  
13 the end;

14 (II) in subparagraph (C)(v), by  
15 striking the period at the end and in-  
16 serting “; and”; and

17 (III) by adding at the end the  
18 following:

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

22 (C) in section 3506—

23 (i) in subsection (a)(3), by inserting  
24 “In carrying out these duties, the Chief In-  
25 formation Officer shall consult, as appro-

1           appropriate, with the Chief Data Officer in ac-  
2           cordance with the designated functions  
3           under section 3520(c).” after “reduction of  
4           information collection burdens on the pub-  
5           lic.”;

6                   (ii) in subsection (b)(1)(C), by insert-  
7           ing “availability,” after “integrity,”;

8                   (iii) in subsection (h)(3), by inserting  
9           “security,” after “efficiency,”; and

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

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

19                   “(A) lead the privacy program of the agency;  
20          and

21                   “(B) carry out the privacy responsibilities of  
22          the agency under this chapter, section 552a of title  
23          5, and guidance issued by the Director.

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

1           “(A) serve in a central leadership position with-  
2           in the agency;

3           “(B) have visibility into relevant agency oper-  
4           ations; and

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

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

13                           (D) in section 3513—

14                                   (i) by redesignating subsection (c) as  
15                                   subsection (d); and

16                                   (ii) by inserting after subsection (b)  
17                                   the following:

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

22                           (2) SUBCHAPTER II DEFINITIONS.—

23                                   (A) IN GENERAL.—Section 3552(b) of title  
24                                   44, United States Code, is amended—

1 (i) by redesignating paragraphs (2),  
2 (3), (4), (5), (6), and (7) as paragraphs  
3 (3), (4), (5), (6), (8), and (10), respec-  
4 tively;

5 (ii) by inserting after paragraph (1)  
6 the following:

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

17 (iii) by inserting after paragraph (6),  
18 as so redesignated, the following:

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

22 (iv) in paragraph (8)(A), as so redesi-  
23 gnated, in the matter preceding clause (i),  
24 by striking “used” and inserting “owned,  
25 managed,”;

1 (v) by inserting after paragraph (8),  
2 as so redesignated, the following:

3 “(9) The term ‘penetration test’—

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

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

13 (vi) by inserting after paragraph (10),  
14 as so redesignated, the following:

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

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

23 (B) CONFORMING AMENDMENTS.—

24 (i) HOMELAND SECURITY ACT OF  
25 2002.—Section 1001(e)(1)(A) of the Home-

1 land Security Act of 2002 (6 U.S.C.  
2 511(c)(1)(A)) is amended by striking “sec-  
3 tion 3552(b)(5)” and inserting “section  
4 3552(b)”.

5 (ii) TITLE 10.—

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

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

16 (III) SECTION 3068.—Section  
17 3068(b) of title 10, United States  
18 Code, is amended by striking “section  
19 3552(b)(6)” and inserting “section  
20 3552(b)”.

21 (IV) SECTION 3252.—Section  
22 3252(e)(5) of title 10, United States  
23 Code, is amended by striking “section  
24 3552(b)(6)” and inserting “section  
25 3552(b)”.



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

7 (iv) INTERNET OF THINGS CYBERSE-  
8 CURITY IMPROVEMENT ACT OF 2020.—Sec-  
9 tion 3(5) of the Internet of Things Cyber-  
10 security Improvement Act of 2020 (15  
11 U.S.C. 278g–3a(5)) is amended by striking  
12 “section 3552(b)(6)” and inserting “sec-  
13 tion 3552(b)”.

14 (v) NATIONAL DEFENSE AUTHORIZA-  
15 TION ACT FOR FISCAL YEAR 2013.—Section  
16 933(e)(1)(B) of the National Defense Au-  
17 thorization Act for Fiscal Year 2013 (10  
18 U.S.C. 2224 note) is amended by striking  
19 “section 3542(b)(2)” and inserting “sec-  
20 tion 3552(b)”.

21 (vi) IKE SKELTON NATIONAL DE-  
22 FENSE AUTHORIZATION ACT FOR FISCAL  
23 YEAR 2011.—The Ike Skelton National De-  
24 fense Authorization Act for Fiscal Year  
25 2011 (Public Law 111–383) is amended—

1 (I) in section 931(b)(3) (10  
2 U.S.C. 2223 note), by striking “sec-  
3 tion 3542(b)(2)” and inserting “sec-  
4 tion 3552(b)”;

5 (II) in section 932(b)(2) (10  
6 U.S.C. 2224 note), by striking “sec-  
7 tion 3542(b)(2)” and inserting “sec-  
8 tion 3552(b)”.

9 (vii) E-GOVERNMENT ACT OF 2002.—  
10 Section 301(c)(1)(A) of the E-Government  
11 Act of 2002 (44 U.S.C. 3501 note) is  
12 amended by striking “section 3542(b)(2)”  
13 and inserting “section 3552(b)”.

14 (viii) NATIONAL INSTITUTE OF  
15 STANDARDS AND TECHNOLOGY ACT.—Sec-  
16 tion 20 of the National Institute of Stand-  
17 ards and Technology Act (15 U.S.C. 278g-  
18 3) is amended—

19 (I) in subsection (a)(2), by strik-  
20 ing “section 3552(b)(6)” and insert-  
21 ing “section 3552(b)”;

22 (II) in subsection (f)—

23 (aa) in paragraph (2), by  
24 striking “section 3532(1)” and  
25 inserting “section 3552(b)”;

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

4 (3) SUBCHAPTER II AMENDMENTS.—Sub-  
5 chapter II of chapter 35 of title 44, United States  
6 Code, is amended—

7 (A) in section 3551—

8 (i) in paragraph (4), by striking “di-  
9 agnose and improve” and inserting “inte-  
10 grate, deliver, diagnose, and improve”;

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

13 (iii) in paragraph (6), by striking the  
14 period at the end and inserting a semi-  
15 colon; and

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

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

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

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

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

6 (B) in section 3553—

7 (i) in subsection (a)—

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

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

13 (III) by adding at the end the  
14 following:

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

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

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

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

4 (ii) in subsection (b)—

5 (I) in the matter preceding para-  
6 graph (1), by inserting “and the Na-  
7 tional Cyber Director” after “Direc-  
8 tor”;

9 (II) in paragraph (2)(A), by in-  
10 sserting “and reporting requirements  
11 under subchapter IV of this chapter”  
12 after “section 3556”;

13 (III) by redesignating paragraphs  
14 (8) and (9) as paragraphs (10) and  
15 (11), respectively; and

16 (IV) by inserting after paragraph  
17 (7) the following:

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

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

3 (iii) in subsection (c)—

4 (I) in the matter preceding para-  
5 graph (1)—

6 (aa) by striking “each year”  
7 and inserting “each year during  
8 which agencies are required to  
9 submit reports under section  
10 3554(c)”;

11 (bb) by inserting “, which  
12 shall be unclassified but may in-  
13 clude 1 or more annexes that  
14 contain classified or other sen-  
15 sitive information, as appro-  
16 priate” after “a report”; and

17 (cc) by striking “preceding  
18 year” and inserting “preceding 2  
19 years”;

20 (II) by striking paragraph (1);

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

1 (IV) in paragraph (3), as so re-  
2 designated, by striking “and” at the  
3 end; and

4 (V) by inserting after paragraph  
5 (3), as so redesignated, the following:

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

9 (iv) in subsection (h)—

10 (I) in paragraph (2)—

11 (aa) in subparagraph (A),  
12 by inserting “and the National  
13 Cyber Director” after “in coordi-  
14 nation with the Director”;

15 (bb) in subparagraph (B),  
16 by inserting “, the scope of the  
17 required action (such as applica-  
18 ble software, firmware, or hard-  
19 ware versions),” after “reasons  
20 for the required action”; and

21 (cc) in subparagraph (D), by  
22 inserting “, the National Cyber  
23 Director,” after “notify the Di-  
24 rector”; and

1 (II) in paragraph (3)(A)(iv), by  
2 inserting “, the National Cyber Direc-  
3 tor” after “the Secretary provides  
4 prior notice to the Director”;  
5 (v) by amending subsection (i) to read  
6 as follows:

7 “(i) FEDERAL RISK ASSESSMENT.—On an ongoing  
8 and continual basis, the Director of the Cybersecurity and  
9 Infrastructure Security Agency shall assess the Federal  
10 risk posture using any available information on the cyber-  
11 security posture of agencies, and brief the Director and  
12 National Cyber Director on the findings of such assess-  
13 ment, 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                         (vi) by adding at the end the fol-  
16                         lowing:

17          “(m) DIRECTIVES.—

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

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

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

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

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

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

1 than 30 days after the issuance of the binding oper-  
2 ational directive, and every 90 days thereafter  
3 until—

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

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

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

13 “(3) REPORT.—If the Director of the Cyberse-  
14 curity and Infrastructure Security Agency ceases  
15 submitting updates required under paragraphs (1)  
16 or (2) on the date described in paragraph (1)(C) or  
17 (2)(C), 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 a list of every agency that, at the  
24 time of the report—

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

3           “(B) has not implemented a binding oper-  
4           ational directive.

5           “(n) REVIEW OF OFFICE OF MANAGEMENT AND  
6 BUDGET GUIDANCE AND POLICY.—

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

14          “(2) CONGRESSIONAL NOTIFICATION.—The Di-  
15          rector of the Office of Management and Budget  
16          shall notify the Committee on Homeland Security  
17          and Governmental Affairs of the Senate and the  
18          Committee on Oversight and Accountability of the  
19          House of Representatives of the results of the review  
20          under paragraph (1).

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

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

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

18                           (C) in section 3554—

19                                   (i) in subsection (a)—

20   (I) in paragraph (1)—

21   (aa) by redesignating sub-  
22 paragraphs (A), (B), and (C) as  
23 subparagraphs (B), (C), and (D),  
24 respectively;

1 (bb) by inserting before sub-  
2 paragraph (B), as so redesign-  
3 nated, the following:

4 “(A) on an ongoing and continual basis,  
5 assessing agency system risk, as applicable,  
6 by—

7 “(i) identifying and documenting the  
8 high value assets of the agency using guid-  
9 ance from the Director;

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

14 “(iii) identifying whether the agency  
15 is participating in federally offered cyber-  
16 security shared services programs;

17 “(iv) identifying agency systems that  
18 have access to or hold the data assets  
19 inventoried under section 3511;

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

1           “(vi) evaluating the vulnerability of  
2           agency systems and data, including high  
3           value assets, including by analyzing—  
4                   “(I) the results of penetration  
5                   testing performed by the Department  
6                   of Homeland Security under section  
7                   3553(b)(9);  
8                   “(II) the results of penetration  
9                   testing performed under section  
10                  3559A;  
11                  “(III) information provided to  
12                  the agency through the vulnerability  
13                  disclosure program of the agency  
14                  under section 3559B;  
15                  “(IV) incidents; and  
16                  “(V) any other vulnerability in-  
17                  formation relating to agency systems  
18                  that is known to the agency;  
19                  “(vii) assessing the impacts of poten-  
20                  tial agency incidents to agency systems,  
21                  data, and operations based on the evalua-  
22                  tions described in clauses (ii) and (v) and  
23                  the agency systems identified under clause  
24                  (iv); and

1           “(viii) assessing the consequences of  
2 potential incidents occurring on agency  
3 systems that would impact systems at  
4 other agencies, including due to  
5 interconnectivity between different agency  
6 systems or operational reliance on the op-  
7 erations of the system or data in the sys-  
8 tem;”;

9                         (cc) in subparagraph (B), as  
10 so redesignated, in the matter  
11 preceding clause (i), by striking  
12 “providing information” and in-  
13 serting “using information from  
14 the assessment required under  
15 subparagraph (A), providing in-  
16 formation”;

17                         (dd) in subparagraph (C), as  
18 so redesignated—

19                                 (AA) in clause (ii) by  
20 inserting “binding” before  
21 “operational”; and

22                                 (BB) in clause (vi), by  
23 striking “and” at the end;

24                         (ee) in subparagraph (D), as  
25 so redesignated, by inserting



1 “and” after the semicolon at the  
2 end; and

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

5 “(E) providing an update on the ongoing  
6 and continual assessment required under sub-  
7 paragraph (A)—

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

11 “(ii) at intervals determined by guid-  
12 ance issued by the Director, and to the ex-  
13 tent appropriate and practicable using au-  
14 tomation, to—

15 “(I) the Director;

16 “(II) the Director of the Cyberse-  
17 curity and Infrastructure Security  
18 Agency; and

19 “(III) the National Cyber Direc-  
20 tor;”;

21 (II) in paragraph (2)—

22 (aa) in subparagraph (A),  
23 by inserting “in accordance with  
24 the agency system risk assess-  
25 ment required under paragraph

1 (1)(A)” after “information sys-  
2 tems”; and

3 (bb) in subparagraph (D),  
4 by inserting “, through the use of  
5 penetration testing, the vulner-  
6 ability disclosure program estab-  
7 lished under section 3559B, and  
8 other means,” after “periodi-  
9 cally”;

10 (III) in paragraph (3)(A)—

11 (aa) in the matter preceding  
12 clause (i), by striking “senior  
13 agency information security offi-  
14 cer” and inserting “Chief Infor-  
15 mation Security Officer”;

16 (bb) in clause (i), by striking  
17 “this section” and inserting  
18 “subsections (a) through (c)”;

19 (cc) in clause (ii), by strik-  
20 ing “training and” and inserting  
21 “skills, training, and”;

22 (dd) by redesignating  
23 clauses (iii) and (iv) as clauses  
24 (iv) and (v), respectively;

1 (ee) by inserting after clause

2 (ii) the following:

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

8 (ff) in clause (iv), as so re-  
9 designated, by striking “informa-  
10 tion security duties as that offi-  
11 cial’s primary duty” and insert-  
12 ing “information, computer net-  
13 work, and technology security du-  
14 ties as the Chief Information Se-  
15 curity Officers’ primary duty”;

16 (IV) in paragraph (5), by strik-  
17 ing “annually” and inserting “not less  
18 frequently than quarterly”; and

19 (V) in paragraph (6), by striking  
20 “official delegated” and inserting  
21 “Chief Information Security Officer  
22 delegated”;

23 (ii) in subsection (b)—

24 (I) by striking paragraph (1) and  
25 inserting the following:

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

7 (II) in paragraph (2)—

8 (aa) by striking subpara-  
9 graph (B);

10 (bb) by redesignating sub-  
11 paragraphs (C) and (D) as sub-  
12 paragraphs (B) and (C), respec-  
13 tively; and

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

16 (AA) by redesignating  
17 clauses (iii) and (iv) as  
18 clauses (iv) and (v), respec-  
19 tively;

20 (BB) by inserting after  
21 clause (ii) the following:

22 “(iii) binding operational directives  
23 and emergency directives issued by the  
24 Secretary under section 3553;” and

1 (CC) in clause (iv), as  
2 so redesignated, by striking  
3 “as determined by the agen-  
4 cy;” and inserting “as deter-  
5 mined by the agency, consid-  
6 ering the agency risk assess-  
7 ment required under sub-  
8 section (a)(1)(A);”;

9 (III) in paragraph (5)(A), by in-  
10 serting “, including penetration test-  
11 ing, as appropriate,” after “shall in-  
12 clude testing”;

13 (IV) by redesignating paragraphs  
14 (7) and (8) as paragraphs (8) and  
15 (9), respectively;

16 (V) by inserting after paragraph  
17 (6) the following:

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

1 (VI) in paragraph (8)(C), as so  
2 redesignated—

3 (aa) by striking clause (ii)  
4 and inserting the following:

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

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

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

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

16 (dd) in clause (iv), as so re-  
17 designated—

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

20 (BB) by striking sub-  
21 clause (III); and

22 (CC) by redesignating  
23 subclause (IV) as subclause  
24 (III); and

25 (iii) in subsection (c)—

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

3 (II) by striking paragraph (1)  
4 and inserting the following:

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

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

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

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

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

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

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



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

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

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

13                               (III) in paragraph (4), as so re-  
14                               designated, by striking the period at  
15                               the end and inserting “, including the  
16                               reporting procedures established  
17                               under section 11315(d) of title 40 and  
18                               subsection (a)(3)(A)(v) of this sec-  
19                               tion.”;

20           (D) in section 3555—

21                               (i) in the section heading, by striking  
22                               “**Annual independent**” and inserting  
23                               “**Independent**”;

24                               (ii) in subsection (a)—

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

5 (II) in paragraph (2)(A), by in-  
6 serting “, including by performing, or  
7 reviewing the results of, agency pene-  
8 tration testing and analyzing the vul-  
9 nerability disclosure program of the  
10 agency” after “information systems”;  
11 and

12 (III) by adding at the end the  
13 following:

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

17 (iii) in subsection (b)(1), by striking  
18 “annual”;

19 (iv) in subsection (e)(1), by inserting  
20 “during which a report is required to be  
21 submitted under section 3553(c)” after  
22 “Each year”;

23 (v) in subsection (g)(2)—

1 (I) by striking “this subsection  
2 shall” and inserting “this sub-  
3 section—

4 “(A) shall”;

5 (II) in subparagraph (A), as so  
6 designated, by striking the period at  
7 the end and inserting “; and”; and

8 (III) by adding at the end the  
9 following:

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

12 (vi) by striking subsection (j) and in-  
13 serting 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           (vii) by adding at the end the fol-  
11 lowing:

12           “(k) COORDINATION.—The head of each agency shall  
13 coordinate with the inspector general of the agency, as ap-  
14 plicable, to ensure consistent understanding of agency cy-  
15 bersecurity or information security policies for the purpose  
16 of evaluations of such policies conducted by the inspector  
17 general.”; and

18           (E) in section 3556(a)—

19           (i) in the matter preceding paragraph  
20 (1), by inserting “within the Cybersecurity  
21 and Infrastructure Security Agency” after  
22 “incident center”; and

23           (ii) in paragraph (4), by striking  
24 “3554(b)” and inserting “3554(a)(1)(A)”.

25           (4) CONFORMING AMENDMENTS.—

1 (A) TABLE OF SECTIONS.—The table of  
2 sections for chapter 35 of title 44, United  
3 States Code, is amended by striking the item  
4 relating to section 3555 and inserting the fol-  
5 lowing:

“3555. Independent evaluation.”.

6 (B) OMB REPORTS.—Section 226(c) of  
7 the Cybersecurity Act of 2015 (6 U.S.C.  
8 1524(c)) is amended—

9 (i) in paragraph (1)(B), in the matter  
10 preceding clause (i), by striking “annually  
11 thereafter” and inserting “thereafter dur-  
12 ing the years during which a report is re-  
13 quired to be submitted under section  
14 3553(c) of title 44, United States Code”;  
15 and

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

18 (I) by striking “annually there-  
19 after” and inserting “thereafter dur-  
20 ing the years during which a report is  
21 required to be submitted under sec-  
22 tion 3553(c) of title 44, United States  
23 Code”; and

24 (II) by striking “the report re-  
25 quired under section 3553(c) of title

1                                   44, United States Code” and inserting  
2                                   “that report”.

3                                   (C) NIST RESPONSIBILITIES.—Section  
4                                   20(d)(3)(B) of the National Institute of Stand-  
5                                   ards and Technology Act (15 U.S.C. 278g-  
6                                   3(d)(3)(B)) is amended by striking “annual”.

7                                   (5) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

11                                  “SUBCHAPTER IV—FEDERAL SYSTEM  
12    INCIDENT RESPONSE

13                                  “**§ 3591. Definitions**

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

17                                  “(b) ADDITIONAL DEFINITIONS.—As used in this  
18                                  subchapter:

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

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

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

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

3           “(D) the Committee on Commerce,  
4 Science, and Transportation of the Senate;

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

7           “(F) the Committee on Homeland Security  
8 of the House of Representatives;

9           “(G) the Committee on Science, Space,  
10 and Technology of the House of Representa-  
11 tives;

12           “(H) the appropriate authorization and ap-  
13 propriations committees of Congress;

14           “(I) the Director;

15           “(J) the Director of the Cybersecurity and  
16 Infrastructure Security Agency;

17           “(K) the National Cyber Director;

18           “(L) the Comptroller General of the  
19 United States; and

20           “(M) the inspector general of any impacted  
21 agency.

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

24           “(A) means—

1                   “(i) the recipient of a grant from an  
2                   agency;

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

5                   “(iii) a party to an other transaction  
6                   agreement with an agency; and

7                   “(B) includes a subawardee of an entity  
8                   described in subparagraph (A).

9                   “(3) BREACH.—The term ‘breach’—

10                   “(A) means the compromise, unauthorized  
11                   disclosure, unauthorized acquisition, or loss of  
12                   control of personally identifiable information  
13                   owned, maintained or otherwise controlled by  
14                   an agency, or any similar occurrence; and

15                   “(B) includes any additional meaning  
16                   given the term in policies, principles, standards,  
17                   or guidelines issued by the Director.

18                   “(4) CONTRACTOR.—The term ‘contractor’  
19                   means a prime contractor of an agency or a subcon-  
20                   tractor of a prime contractor of an agency that cre-  
21                   ates, collects, stores, processes, maintains, or trans-  
22                   mits Federal information on behalf of an agency.

23                   “(5) FEDERAL INFORMATION.—The term ‘Fed-  
24                   eral information’ means information created, col-  
25                   lected, processed, maintained, disseminated, dis-



1 closed, or disposed of by or for the Federal Govern-  
2 ment in any medium or form.

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

8 “(7) INTELLIGENCE COMMUNITY.—The term  
9 ‘intelligence community’ has the meaning given the  
10 term in section 3 of the National Security Act of  
11 1947 (50 U.S.C. 3003).

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

17 “(9) VULNERABILITY DISCLOSURE.—The term  
18 ‘vulnerability disclosure’ means a vulnerability iden-  
19 tified under section 3559B.

20 **“§ 3592. Notification of breach**

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

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

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

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

7                   “(B) the notification is delayed under sub-  
8                   section (d).

9           “(b) NOTIFICATION.—As expeditiously as practicable  
10          and without unreasonable delay, and in any case not later  
11          than 45 days after an agency has a reasonable basis to  
12          conclude that a breach has occurred, the head of the agen-  
13          cy, in consultation with the Chief Information Officer and  
14          Chief Privacy Officer of the agency and, as appropriate,  
15          any non-Federal entity supporting the remediation of the  
16          breach, 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 notifica-  
17          tion of a breach provided to an individual under subsection  
18          (b)(2) shall include, to the maximum extent practicable—

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

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

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

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

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

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

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

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

17          “(d) DELAY OF NOTIFICATION.—

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

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

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

5           “(C) reveal sensitive sources and methods;

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

7           “(E) hamper security remediation actions.

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

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

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

1 “(f) DELAY OF NOTIFICATION REPORT.—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

3               “(1) limit—

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

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

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

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

22                               “(i) the Director;

23                               “(ii) the National Cyber Director;

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

1 “(iv) any other agency;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11         “(b) INITIAL NOTIFICATION.—

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

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

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

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

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

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

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

17                   “(i) the agency;

18                   “(ii) the Federal Government;

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

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

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

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

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

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

3 “(A) the agency;

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

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

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

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

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

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

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

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

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

6 “(7) as appropriate and available, recommenda-  
7 tions for mitigating future similar incidents, includ-  
8 ing recommendations from any non-Federal entity  
9 impacted by or supporting the remediation of the  
10 major incident.

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 congress-  
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 Ac-  
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; and

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;

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) NOTIFICATION.—

1           “(1) IN GENERAL.—Any contractor or awardee  
2 of an agency shall provide written notification to the  
3 agency if the contractor or awardee has a reasonable  
4 basis to conclude 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 a successful exploitation of the vulnerability  
20 by an actor without authorization of the Fed-  
21 eral information system owner; or

22           “(D) the contractor or awardee has re-  
23 ceived from the agency personally identifiable  
24 information or personal health information that  
25 is beyond the scope of the contract or agree-



1           ment with the agency that the contractor or  
2           awardee is not authorized to receive.

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

18           “(3) PROCEDURES.—

19           “(A) SHARING WITH CISA.—As soon as  
20    practicable following a notification of an inci-  
21    dent or vulnerability to an agency by a con-  
22    tractor or awardee under paragraph (1), the  
23    head of the agency shall provide, pursuant to  
24    section 3594, information about the incident or

1 vulnerability to the Director of the Cybersecu-  
2 rity and Infrastructure Security Agency.

3 “(B) TIMING OF NOTIFICATIONS.—Unless  
4 a different time for notification is specified in  
5 a contract, grant, cooperative agreement, or  
6 other transaction agreement, a contractor or  
7 awardee shall—

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

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

21 “(C) PROCEDURES.—Following a notifica-  
22 tion of a breach or incident to an agency by a  
23 contractor 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 notify  
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 as soon as practicable to agencies relating  
12 to the scope of vulnerabilities to be included in re-  
13 quired notifications under paragraph (2), such as  
14 the minimum severity or minimum risk level of a  
15 vulnerability included in required notifications,  
16 whether vulnerabilities that are already publicly dis-  
17 closed must be reported, or likely cybersecurity im-  
18 pact to Federal information systems.

19 “(b) REGULATIONS; MODIFICATIONS.—

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

23 “(A) the Federal Acquisition Regulatory  
24 Council shall promulgate regulations, as appro-  
25 priate, relating to the responsibilities of con-

1 tractors and recipients of other transaction  
2 agreements and cooperative agreements to com-  
3 ply with this section; and

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

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

16 “(3) CONGRESSIONAL NOTIFICATION.—

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

22 “(B) OMB NOTIFICATION.— Not later  
23 than 30 days after the date described in para-  
24 graph (2), the Director shall notify the Com-  
25 mittee on Homeland Security and Govern-

1           mental Affairs of the Senate and the Commit-  
2           tees on Oversight and Accountability and  
3           Homeland Security of the House of Representa-  
4           tives on the status of the implementation by  
5           each agency of the regulations promulgated  
6           under paragraph (1).

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

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

15                 “(2) Identifying—

16                         “(A) a cyber threat (as defined in such  
17                         section 2200), including the source of the cyber  
18                         threat; or

19                         “(B) a security vulnerability (as defined in  
20                         such section 2200).

21                 “(3) Preventing, investigating, disrupting, or  
22                 prosecuting an offense arising out of an incident no-  
23                 tified to an agency pursuant to this section or any  
24                 of the offenses listed in section 105(d)(5)(A)(v) of

1 the Cybersecurity Information Sharing Act of 2015  
2 (6 U.S.C. 1504(d)(5)(A)(v)).

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

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

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

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

6   **“§ 3596. Training**

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

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

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

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

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

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

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

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

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

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

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

17          “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3           “(c) PUBLICATION.—

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

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

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

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

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

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

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

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

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

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

19 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

24 “(2) NONCOMPLIANCE REPORTS.—During any  
25 year during which the head of an agency does not

1 provide data for an incident to the Cybersecurity  
2 and Infrastructure Security Agency in accordance  
3 with section 3594(a), the head of the agency, in co-  
4 ordination with the Director of the Cybersecurity  
5 and Infrastructure Security Agency and the Direc-  
6 tor, shall submit to the appropriate reporting enti-  
7 ties a report that includes the information described  
8 in subsection (b) with respect to the agency.

9 “(e) NATIONAL SECURITY SYSTEM REPORTS.—

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

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

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

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

3           “(D) the Select Committee on Intelligence  
4           of the Senate;

5           “(E) the Committee on Armed Services of  
6           the Senate;

7           “(F) the Committee on Appropriations of  
8           the Senate;

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

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

13          “(I) the Permanent Select Committee on  
14          Intelligence of the House of Representatives;

15          “(J) the Committee on Armed Services of  
16          the House of Representatives; and

17          “(K) the Committee on Appropriations of  
18          the House of Representatives.

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

22       **“§ 3598. Major incident definition**

23          “(a) IN GENERAL.—Not later than 1 year after the  
24          later of the date of enactment of the Federal Information  
25          Security Modernization Act of 2024 and the most recent

1 publication by the Director of guidance to agencies regard-  
2 ing major incidents as of the date of enactment of the  
3 Federal Information Security Modernization Act of 2024,  
4 the Director shall develop, in coordination with the Na-  
5 tional Cyber Director, and promulgate guidance on the  
6 definition of the term ‘major incident’ for the purposes  
7 of subchapter II and this subchapter.

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

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

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

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

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

23 “(B) any incident the head of the agency  
24 determines likely to result in an inability or  
25 substantial disruption for the agency, a compo-



1           nent of the agency, or the Federal Government,  
2           to provide 1 or more critical services;

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

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

13          “(E) any other type of incident determined  
14          appropriate by the Director;

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

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

22                  and

23                  “(B) is enabled by—

24                          “(i) a common technical root cause,  
25                          such as a supply chain compromise, or a

1 common software or hardware vulner-  
2 ability; or

3 “(ii) the related activities of a com-  
4 mon threat actor;

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

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

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

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

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

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

6                   (B) CLERICAL AMENDMENT.—The table of  
7           sections for chapter 35 of title 44, United  
8           States Code, is amended by adding at the end  
9           the following:

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification of breach.

“3593. Congressional and executive branch reports on major incidents.

“3594. Government information sharing and incident response.

“3595. Responsibilities of contractors and awardees.

“3596. Training.

“3597. Analysis and report on Federal incidents.

“3598. Major incident definition.”.

10           (b) AMENDMENTS TO SUBTITLE III OF TITLE 40.—

11                   (1) MODERNIZING GOVERNMENT TECH-  
12           NOLOGY.—Subtitle G of title X of division A of the  
13           National Defense Authorization Act for Fiscal Year  
14           2018 (40 U.S.C. 11301 note) is amended in section  
15           1078—

16                   (A) by striking subsection (a) and insert-  
17           ing the following:

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

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

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

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

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

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

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

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

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

21           (C) in subsection (c)—

22           (i) in paragraph (2)(A)(i), by insert-  
23 ing “, including a consideration of the im-  
24 pact on high value assets” after “oper-  
25 ational risks”;

1 (ii) in paragraph (5)—

2 (I) in subparagraph (A), by strik-  
3 ing “and” at the end;

4 (II) in subparagraph (B), by  
5 striking the period at the end and in-  
6 serting “; and”; and

7 (III) by adding at the end the  
8 following:

9 “(C) a senior official from the Cybersecu-  
10 rity and Infrastructure Security Agency of the  
11 Department of Homeland Security, appointed  
12 by the Director.”; and

13 (iii) in paragraph (6)(A), by striking  
14 “shall be—” and all that follows through  
15 “4 employees” and inserting “shall be 4  
16 employees”.

17 (2) SUBCHAPTER I.—Subchapter I of chapter  
18 113 of subtitle III of title 40, United States Code,  
19 is amended—

20 (A) in section 11302—

21 (i) in subsection (b), by striking “use,  
22 security, and disposal of” and inserting  
23 “use, and disposal of, and, in consultation  
24 with the Director of the Cybersecurity and  
25 Infrastructure Security Agency and the

1 National Cyber Director, promote and im-  
2 prove the security of,”; and

3 (ii) in subsection (h), by inserting “,  
4 including cybersecurity performances,”  
5 after “the performances”; and

6 (B) in section 11303(b)(2)(B)—

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

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

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

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

16 (3) SUBCHAPTER II.—Subchapter II of chapter  
17 113 of subtitle III of title 40, United States Code,  
18 is amended—

19 (A) in section 11312(a), by inserting “, in-  
20 cluding security risks” after “managing the  
21 risks”;

22 (B) in section 11313(1), by striking “effi-  
23 ciency and effectiveness” and inserting “effi-  
24 ciency, security, and effectiveness”;

1 (C) in section 11317, by inserting “secu-  
2 rity,” before “or schedule”; and

3 (D) in section 11319(b)(1), in the para-  
4 graph heading, by striking “CIOS” and inserting  
5 “CHIEF INFORMATION OFFICERS”.

6 (c) ACTIONS TO ENHANCE FEDERAL INCIDENT  
7 TRANSPARENCY.—

8 (1) RESPONSIBILITIES OF THE CYBERSECURITY  
9 AND INFRASTRUCTURE SECURITY AGENCY.—

10 (A) IN GENERAL.—Not later than 180  
11 days after the date of enactment of this section,  
12 the Director of the Cybersecurity and Infra-  
13 structure Security Agency shall—

14 (i) develop a plan for the development,  
15 using systems in place on the date of en-  
16 actment of this section, of the analysis re-  
17 quired under section 3597(a) of title 44,  
18 United States Code, as added by this  
19 sectuib, and the report required under sub-  
20 section (b) of that section that includes—

21 (I) a description of any chal-  
22 lenges the Director of the Cybersecu-  
23 rity and Infrastructure Security Agen-  
24 cy anticipates encountering; and

1 (II) the use of automation and  
2 machine-readable formats for col-  
3 lecting, compiling, monitoring, and  
4 analyzing data; and

5 (ii) provide to the appropriate con-  
6 gressional committees a briefing on the  
7 plan developed under clause (i).

8 (B) BRIEFING.—Not later than 1 year  
9 after the date of enactment of this section, the  
10 Director of the Cybersecurity and Infrastruc-  
11 ture Security Agency shall provide to the appro-  
12 priate congressional committees a briefing on—

13 (i) the execution of the plan required  
14 under subparagraph (A)(i); and

15 (ii) the development of the report re-  
16 quired under section 3597(b) of title 44,  
17 United States Code, as added by this sec-  
18 tion.

19 (2) RESPONSIBILITIES OF THE DIRECTOR OF  
20 THE OFFICE OF MANAGEMENT AND BUDGET.—

21 (A) UPDATING FISMA 2014.—Section 2 of  
22 the Federal Information Security Modernization  
23 Act of 2014 (Public Law 113–283; 128 Stat.  
24 3073) is amended—



1 (i) by striking subsections (b) and (d);

2 and

3 (ii) by redesignating subsections (c),

4 (e), and (f) as subsections (b), (c), and (d),

5 respectively.

6 (B) INCIDENT DATA SHARING.—

7 (i) IN GENERAL.—The Director, in co-  
8 ordination with the Director of the Cyber-  
9 security and Infrastructure Security Agen-  
10 cy, shall develop, and as appropriate up-  
11 date, guidance, on the content, timeliness,  
12 and format of the information provided by  
13 agencies under section 3594(a) of title 44,  
14 United States Code, as added by this sec-  
15 tion.

16 (ii) REQUIREMENTS.—The guidance  
17 developed under clause (i) shall—

18 (I) enable the efficient develop-  
19 ment of—

20 (aa) lessons learned and rec-  
21 ommendations in responding to,  
22 recovering from, remediating,  
23 and mitigating future incidents;  
24 and

1 (bb) the report on Federal  
2 incidents required under section  
3 3597(b) of title 44, United  
4 States Code, as added by this  
5 section; and

6 (II) include requirements for the  
7 timeliness of data production.

8 (iii) AUTOMATION.—The Director, in  
9 coordination with the Director of the Cy-  
10 bersecurity and Infrastructure Security  
11 Agency, shall promote, as feasible, the use  
12 of automation and machine-readable data  
13 for data sharing under section 3594(a) of  
14 title 44, United States Code, as added by  
15 this section.

16 (C) CONTRACTOR AND AWARDEE GUID-  
17 ANCE.—

18 (i) IN GENERAL.—Not later than 1  
19 year after the date of enactment of this  
20 section, the Director shall issue guidance  
21 to agencies on how to deconflict, to the  
22 greatest extent practicable, existing regula-  
23 tions, policies, and procedures relating to  
24 the responsibilities of contractors and  
25 awardees established under section 3595 of

1 title 44, United States Code, as added by  
2 this section.

3 (ii) EXISTING PROCESSES.—To the  
4 greatest extent practicable, the guidance  
5 issued under clause (i) shall allow contrac-  
6 tors and awardees to use existing processes  
7 for notifying agencies of incidents involving  
8 information of the Federal Government.

9 (3) UPDATE TO THE PRIVACY ACT OF 1974.—  
10 Section 552a(b) of title 5, United States Code (com-  
11 monly known as the “Privacy Act of 1974”) is  
12 amended—

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

15 (B) in paragraph (12), by striking the pe-  
16 riod at the end and inserting “; or”; and

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

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

24 (d) AGENCY REQUIREMENTS TO NOTIFY PRIVATE  
25 SECTOR ENTITIES IMPACTED BY INCIDENTS.—

1           (1) GUIDANCE ON NOTIFICATION OF REPORT-  
2           ING ENTITIES.—Not later than 1 year after the date  
3           of enactment of this section, the Director shall de-  
4           velop, in consultation with the National Cyber Direc-  
5           tor, and issue guidance requiring the head of each  
6           agency to notify a reporting entity in an appropriate  
7           and timely manner, and take into consideration the  
8           need to coordinate with Sector Risk Management  
9           Agencies (as defined in section 2200 of the Home-  
10          land Security Act of 2002 (6 U.S.C. 650)), as ap-  
11          propriate, of an incident at the agency that is likely  
12          to substantially affect—

13                 (A) the confidentiality or integrity of sen-  
14                 sitive information submitted by the reporting  
15                 entity to the agency pursuant to a statutory or  
16                 regulatory requirement; or

17                 (B) any information system (as defined in  
18                 section 3502 of title 44, United States Code)  
19                 used in the transmission or storage of the sen-  
20                 sitive information described in subparagraph  
21                 (A).

22          (2) DEFINITIONS.—In this subsection:

23                 (A) REPORTING ENTITY.—The term “re-  
24                 porting entity” means private organization or  
25                 governmental unit that is required by statute or

1 regulation to submit sensitive information to an  
2 agency.

3 (B) SENSITIVE INFORMATION.—The term  
4 “sensitive information” has the meaning given  
5 the term by the Director in guidance issued  
6 under paragraph (1).

7 (e) FEDERAL PENETRATION TESTING POLICY.—

8 (1) IN GENERAL.—Subchapter II of chapter 35  
9 of title 44, United States Code, is amended by add-  
10 ing at the end the following:

11 **“§ 3559A. Federal penetration testing**

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

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

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

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

22 “(B) procedures to use the results of pene-  
23 tration testing to improve the cybersecurity and  
24 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, or  
7           penetration testing under this chapter.

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

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

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

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

18                 (2) EXISTING GUIDANCE.—

19                         (A) IN GENERAL.—Compliance with guid-  
20                         ance issued by the Director relating to penetra-  
21                         tion testing before the date of enactment of this  
22                         section shall be deemed to be compliant with  
23                         section 3559A of title 44, United States Code,  
24                         as added by this section.

1 (B) IMMEDIATE NEW GUIDANCE NOT RE-  
2 QUIRED.—Nothing in section 3559A of title 44,  
3 United States Code, as added by this section,  
4 shall be construed to require the Director to  
5 issue new guidance to agencies relating to pene-  
6 tration testing before the date described in  
7 clause (iii).

8 (C) GUIDANCE UPDATES.—Notwith-  
9 standing clauses (i) and (ii), not later than 2  
10 years after the date of enactment of this sec-  
11 tion, the Director shall review and, as appro-  
12 priate, update existing guidance requiring pene-  
13 tration testing by agencies.

14 (3) CLERICAL AMENDMENT.—The table of sec-  
15 tions for chapter 35 of title 44, United States Code,  
16 is amended by adding after the item relating to sec-  
17 tion 3559 the following:

“3559A. Federal penetration testing.”.

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

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

1           “(A) without consent or authorization from  
2 agencies; and

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

6 (f) VULNERABILITY DISCLOSURE POLICIES.—

7           (1) IN GENERAL.—Chapter 35 of title 44,  
8 United States Code, is amended by inserting after  
9 section 3559A, as added by this section, the fol-  
10 lowing:

11 **“§ 3559B. Federal vulnerability disclosure policies**

12           “(a) PURPOSE; SENSE OF CONGRESS.—

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

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

23           “(b) DEFINITIONS.—In this section:

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



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

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

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

16           “(5) VULNERABILITY DISCLOSURE REPORT.—  
17 The term ‘vulnerability disclosure report’ means a  
18 disclosure of a security vulnerability made to an  
19 agency by a submitter.

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

22           “(1) use of the information system security  
23 vulnerabilities disclosure process guidelines estab-  
24 lished under section 4(a)(1) of the IoT Cybersecurity

1 Improvement Act of 2020 (15 U.S.C. 278g–  
2 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 ef-  
10 fort to follow the vulnerability disclosure policy  
11 of the 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  
24 by a submitter of a security vulnerability, without a  
25 significant compromise of confidentiality, integrity,

1 or availability, does not constitute a major incident;  
2 and

3 “(7) the applicability of the guidance to inter-  
4 net of things devices owned or controlled by an  
5 agency.

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

10 “(e) RESPONSIBILITIES OF CISA.—The Director of  
11 the Cybersecurity and Infrastructure Security Agency  
12 shall—

13 “(1) provide support to agencies with respect to  
14 the implementation of the requirements of this sec-  
15 tion;

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

20 “(3) upon a request by an agency, assist the  
21 agency in the disclosure to vendors of newly identi-  
22 fied security vulnerabilities in vendor products and  
23 services; and

24 “(4) as appropriate, implement the require-  
25 ments of this section, in accordance with the author-

1           ity under section 3553(b)(8), as a shared service  
2           available to agencies.

3           “(f) RESPONSIBILITIES OF AGENCIES.—

4                   “(1) PUBLIC INFORMATION.—The head of each  
5           agency shall make publicly available, with respect to  
6           each internet domain under the control of the agen-  
7           cy that is not a national security system and to the  
8           extent consistent with the security of information  
9           systems but with the presumption of disclosure—

10                           “(A) an appropriate security contact; and

11                           “(B) the component of the agency that is  
12           responsible for the internet accessible services  
13           offered at the domain.

14                   “(2) VULNERABILITY DISCLOSURE POLICY.—

15           The head of each agency shall develop and make  
16           publicly available a vulnerability disclosure policy for  
17           the agency, which shall—

18                           “(A) describe—

19                                   “(i) the scope of the systems of the  
20           agency included in the vulnerability disclo-  
21           sure policy, including for internet of things  
22           devices owned or controlled by the agency;

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

1 “(iii) the type of information system  
2 testing that is not authorized by the agen-  
3 cy;

4 “(iv) the disclosure policy for a con-  
5 tractor; and

6 “(v) the disclosure policy of the agen-  
7 cy for sensitive information;

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

10 “(i) how the submitter should submit  
11 the vulnerability disclosure report; and

12 “(ii) if the report is not anonymous,  
13 when the reporter should anticipate an ac-  
14 knowledgment of receipt of the report by  
15 the agency;

16 “(C) include any other relevant informa-  
17 tion; and

18 “(D) be mature in scope and cover every  
19 internet accessible information system used or  
20 operated by that agency or on behalf of that  
21 agency.

22 “(3) IDENTIFIED SECURITY  
23 VULNERABILITIES.—The head of each agency  
24 shall—

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

3           “(B) commensurate with the risk posed by  
4           the security vulnerability, address such security  
5           vulnerability using the security vulnerability  
6           management process of the agency; and

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

10          “(g) EXEMPTIONS.—

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

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

23           “(A) disrupt a law enforcement investiga-  
24           tion;

1           “(B) endanger national security or intel-  
2           ligence activities; or

3           “(C) impede national defense activities or  
4           military operations.

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

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

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

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

15           “(i) REVISION OF FEDERAL ACQUISITION REGULA-  
16           TION.—The Federal Acquisition Regulation shall be re-  
17           vised as necessary to implement the provisions under this  
18           section.”.

19           (2) EXISTING GUIDANCE AND POLICIES.—

20           (A) IN GENERAL.—Compliance with guid-  
21           ance issued by the Director relating to vulner-  
22           ability disclosure policies before the date of en-  
23           actment of this section shall be deemed to be  
24           compliance with section 3559B of title 44,  
25           United States Code, as added by this section.

1 (B) IMMEDIATE NEW GUIDANCE NOT RE-  
2 QUIRED.—Nothing in section 3559B of title 44,  
3 United States Code, as added by this title, shall  
4 be construed to require the Director to issue  
5 new guidance to agencies relating to vulner-  
6 ability disclosure policies before the date de-  
7 scribed in paragraph (4).

8 (C) IMMEDIATE NEW POLICIES NOT RE-  
9 QUIRED.—Nothing in section 3559B of title 44,  
10 United States Code, as added by this title, shall  
11 be construed to require the head of any agency  
12 to issue new policies relating to vulnerability  
13 disclosure policies before the issuance of any  
14 updated guidance under paragraph (4).

15 (D) GUIDANCE UPDATE.—Notwithstanding  
16 paragraphs (1), (2) and (3), not later than 4  
17 years after the date of enactment of this sec-  
18 tion, the Director shall review and, as appro-  
19 priate, update existing guidance relating to vul-  
20 nerability disclosure policies.

21 (3) CLERICAL AMENDMENT.—The table of sec-  
22 tions for chapter 35 of title 44, United States Code,  
23 is amended by adding after the item relating to sec-  
24 tion 3559A, as added by this section, the following:

“3559B. Federal vulnerability disclosure policies.”.

25 (4) CONFORMING UPDATE AND REPEAL.—



1 (A) GUIDELINES ON THE DISCLOSURE  
2 PROCESS FOR SECURITY VULNERABILITIES RE-  
3 LATING TO INFORMATION SYSTEMS, INCLUDING  
4 INTERNET OF THINGS DEVICES.—Section 5 of  
5 the IoT Cybersecurity Improvement Act of  
6 2020 (15 U.S.C. 278g–3e) is amended by strik-  
7 ing subsections (d) and (e).

8 (B) IMPLEMENTATION AND CONTRACTOR  
9 COMPLIANCE.—The IoT Cybersecurity Improve-  
10 ment Act of 2020 (15 U.S.C. 278g–3a et seq.)  
11 is amended—

12 (i) by striking section 6 (15 U.S.C.  
13 278g–3d); and

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

16 (g) IMPLEMENTING ZERO TRUST ARCHITECTURE.—

17 (1) BRIEFINGS.—Not later than 1 year after  
18 the date of enactment of this section, the Director  
19 shall provide to the Committee on Homeland Secu-  
20 rity and Governmental Affairs of the Senate and the  
21 Committees on Oversight and Accountability and  
22 Homeland Security of the House of Representatives  
23 a briefing on progress in increasing the internal de-  
24 fenses of agency systems, including—

1 (A) shifting away from trusted networks to  
2 implement security controls based on a pre-  
3 sumption of compromise, including through the  
4 transition to zero trust architecture;

5 (B) implementing principles of least privi-  
6 lege in administering information security pro-  
7 grams;

8 (C) limiting the ability of entities that  
9 cause incidents to move laterally through or be-  
10 tween agency systems;

11 (D) identifying incidents quickly;

12 (E) isolating and removing unauthorized  
13 entities from agency systems as quickly as prac-  
14 ticable, accounting for intelligence or law en-  
15 forcement purposes; and

16 (F) otherwise increasing the resource costs  
17 for entities that cause incidents to be success-  
18 ful.

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

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

3 (A) a description of steps agencies have  
4 completed, including progress toward achieving  
5 any requirements issued by the Director, in-  
6 cluding the adoption of any models or reference  
7 architecture;

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

11 (C) a schedule to implement any planned  
12 activities.

13 (3) CLASSIFIED ANNEX.—Each update required  
14 under paragraph (2) may include 1 or more annexes  
15 that contain classified or other sensitive information,  
16 as appropriate.

17 (4) NATIONAL SECURITY SYSTEMS.—

18 (A) BRIEFING.—Not later than 1 year  
19 after the date of enactment of this section, the  
20 Secretary of Defense shall provide to the Com-  
21 mittee on Homeland Security and Govern-  
22 mental Affairs of the Senate, the Committee on  
23 Oversight and Accountability of the House of  
24 Representatives, the Committee on Armed Serv-  
25 ices of the Senate, the Committee on Armed

1 Services of the House of Representatives, the  
2 Select Committee on Intelligence of the Senate,  
3 and the Permanent Select Committee on Intel-  
4 ligence of the House of Representatives a brief-  
5 ing on the implementation of zero trust archi-  
6 tecture with respect to national security sys-  
7 tems.

8 (B) PROGRESS REPORT.—Not later than  
9 the date on which each update is required to be  
10 submitted under paragraph (2), the Secretary  
11 of Defense shall submit to the congressional  
12 committees described in subparagraph (A) a  
13 progress report on the implementation of zero  
14 trust architecture with respect to national secu-  
15 rity systems.

16 (h) AUTOMATION AND ARTIFICIAL INTELLIGENCE.—

17 (1) USE OF ARTIFICIAL INTELLIGENCE.—

18 (A) IN GENERAL.—As appropriate, the Di-  
19 rector shall issue guidance on the use of artifi-  
20 cial intelligence by agencies to improve the cy-  
21 bersecurity of information systems.

22 (B) CONSIDERATIONS.—The Director and  
23 head of each agency shall consider the use and  
24 capabilities of artificial intelligence systems in

1 furtherance of the cybersecurity of information  
2 systems.

3 (C) REPORT.—Not later than 1 year after  
4 the date of enactment of this section, and annu-  
5 ally thereafter until the date that is 5 years  
6 after the date of enactment of this section, the  
7 Director shall submit to the appropriate con-  
8 gressional committees a report on the use of ar-  
9 tificial intelligence to further the cybersecurity  
10 of information systems.

11 (2) COMPTROLLER GENERAL REPORTS.—

12 (A) IN GENERAL.—Not later than 2 years  
13 after the date of enactment of this section, the  
14 Comptroller General of the United States shall  
15 submit to the appropriate congressional com-  
16 mittees a report on the risks to the privacy of  
17 individuals and the cybersecurity of information  
18 systems associated with the use by Federal  
19 agencies of artificial intelligence systems or ca-  
20 pabilities.

21 (B) STUDY.—Not later than 2 years after  
22 the date of enactment of this section, the  
23 Comptroller General of the United States shall  
24 perform a study, and submit to the Committees  
25 on Homeland Security and Governmental Af-

1           fairs and Commerce, Science, and Transpor-  
2           tation of the Senate and the Committees on  
3           Oversight and Accountability, Homeland Secu-  
4           rity, and Science, Space, and Technology of the  
5           House of Representatives a report, on the use  
6           of automation, artificial intelligence, including  
7           generative artificial intelligence, and machine-  
8           readable data across the Federal Government  
9           for cybersecurity purposes, including—

10                   (i) the automated updating of cyberse-  
11                   curity tools, sensors, or processes employed  
12                   by agencies under paragraphs (1), (5)(C),  
13                   and (8)(B) of section 3554(b) of title 44,  
14                   United States Code, as amended by this  
15                   section; and

16                   (ii) to combat social engineering at-  
17                   tacks.

18           (3) INFORMATION SYSTEM DEFINED.—In this  
19           subsection, the term “information system” has the  
20           meaning given the term in section 3502 of title 44,  
21           United States Code.

22           (i) FEDERAL CYBERSECURITY REQUIREMENTS.—

23                   (1) CODIFYING FEDERAL CYBERSECURITY RE-  
24                   QUIREMENTS IN TITLE 44.—

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

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

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

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

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

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

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

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

3 “(D) implement identity and access man-  
4 agement systems to ensure the security of Fed-  
5 eral information systems and protect agency  
6 records and data from fraud resulting from the  
7 misrepresentation of identity or identity theft,  
8 including—

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

23 “(ii) multi-factor authentication, con-  
24 sistent with guidance issued by the Direc-  
25 tor of the Office of Management and



1           Budget who shall consider any applicable  
2           standard or guideline developed by the Na-  
3           tional Institute of Standards and Tech-  
4           nology, for—

5                   “(I) remote access to an informa-  
6                   tion system; and

7                   “(II) each user account with ele-  
8                   vated privileges on an information  
9                   system.

10           “(2) PROHIBITION.—

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

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

1 vice prevents compliance with the standards  
2 and guidelines developed under section 4 of the  
3 IoT Cybersecurity Improvement Act (15 U.S.C.  
4 278g–3b) with respect to the device.

5 “(3) EXCEPTIONS.—

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

11 “(i) certified to the Director with par-  
12 ticularity that—

13 “(I) operational requirements ar-  
14 ticulated in the certification and re-  
15 lated to the information system would  
16 make it excessively burdensome to im-  
17 plement the cybersecurity require-  
18 ment;

19 “(II) the cybersecurity require-  
20 ment is not necessary to secure the  
21 information system or agency infor-  
22 mation stored on or transiting it; and

23 “(III) the agency has taken all  
24 necessary steps to secure the informa-

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

3                   “(ii) submitted the certification de-  
4                   scribed in clause (i) to the appropriate con-  
5                   gressional committees and the authorizing  
6                   committees of the agency.

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

15                  “(i) without delegation—

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

24                  “(II) with regard to a system or  
25                  platform in use as of the date of en-

1 actment of this subsection, the head  
2 of the agency provides such certifi-  
3 cation to the Director within 60 days  
4 after the date of enactment of this  
5 subsection;

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

9 “(iii) has submitted the certification  
10 described in clause (i) and the waiver de-  
11 scribed clause (ii) to the appropriate con-  
12 gressional committees and the authorizing  
13 committees of the agency.

14 “(4) DURATION OF CERTIFICATION.—

15 “(A) IN GENERAL.—A certification and  
16 corresponding exemption of an agency under  
17 paragraph (3) shall expire on the date that is  
18 4 years after the date on which the head of the  
19 agency submits the certification under para-  
20 graph (3).

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

1           “(5) PRESUMPTION OF ADEQUACY.—A  
2 FedRAMP authorization issued pursuant to chapter  
3 36 of title 44 shall be presumed adequate to fulfill  
4 the requirements under subparagraphs (A) through  
5 (C) of paragraph (1) with respect to an agency au-  
6 thorization to operate cloud computing products and  
7 services if such presumption of adequacy does not  
8 alter or modify—

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

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

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

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

1 “(B) to affect the standards or process of  
2 the National Institute of Standards and Tech-  
3 nology;

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

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

10 “(E) to affect the requirements under sub-  
11 chapter III.

12 “(g) EXCEPTION.—

13 “(1) NATIONAL SECURITY SYSTEM REQUIRE-  
14 MENTS.—The requirements under subsection (f)(1)  
15 shall not apply to—

16 “(A) a national security system; or

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

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

21 “(A) necessary in the interest of national  
22 security;

23 “(B) national security systems; or

24 “(C) a procured internet of things device  
25 described in subsection (f)(2)(B) that the Chief

1 Information Officer of an agency determines  
2 is—

3 “(i) necessary for research purposes;

4 “(ii) necessary in the interest of na-  
5 tional security; or

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

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

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

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

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

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

23 (3) GUIDANCE FOR IDENTITY MANAGEMENT  
24 SYSTEMS USED BY AGENCIES.—Not later than 1  
25 year after the date of enactment of this section, the

1 Director of the Office of Management and Budget,  
2 in consultation with the Director of the National In-  
3 stitute of Standards and Technology, shall issue,  
4 and routinely update thereafter, guidance for agen-  
5 cies to implement identity management systems and  
6 a single sign-on trusted identity platform as required  
7 under section 3554(f)(1)(D)(i) of title 44, United  
8 States Code, as amended by this section, which shall  
9 at a minimum, include the following:

10 (A) Requirements for agencies to routinely  
11 certify that such systems are in compliance with  
12 this guidance.

13 (B) Requirements for agencies to routinely  
14 verify and certify that information stored on or  
15 transiting through a commercially available  
16 product (as defined in section 103 of title 41,  
17 United States Code) or commercial service (as  
18 defined in section 103a of title 41, United  
19 States Code) used to fulfil such requirements is  
20 appropriately secured in conformity with sub-  
21 chapter II of chapter 35 of title 44, United  
22 States Code.

23 (C) Address national security concerns and  
24 requirements to ensure the protection of sen-  
25 sitive personal records and biometric data of



1 United States persons from malign foreign own-  
2 ership, control, or influence and fraud actors.

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

6 (E) Requirements to prevent discrimina-  
7 tion in violation of title VI of the Civil Rights  
8 Act of 1964 (42 U.S.C. 2000d et seq.).

9 (F) A description of the information nec-  
10 essary to be submitted under the exception de-  
11 scribed in section 3554(f)(3)(B) of title 44,  
12 United States Code, as amended by this sec-  
13 tion.

14 (4) GAO EVALUATION OF TECHNICAL CAPA-  
15 BILITY OF IDENTITY MANAGEMENT SYSTEMS AND  
16 PLATFORMS.—Not less frequently than every 3 years  
17 for the next 6 years after the date of the enactment  
18 of this section, the Comptroller General shall submit  
19 to the appropriate congressional committees a report  
20 on whether the single sign-on trusted identity sys-  
21 tems and platforms used by agencies or the one de-  
22 veloped by the General Services Administration  
23 under section 3554(f)(D)(i) of title 44, United  
24 States Code, as amended by this section, adhere to  
25 the information security requirements of chapter 35

1 of title 44, United States Code, guidance issued  
2 under subparagraph (C), and relevant identity man-  
3 agement technical standards promulgated by the Na-  
4 tional Institute of Standards and Technology, as ap-  
5 propriate, including section 504 of the Cybersecurity  
6 Enhancement Act of 2014 (15 U.S.C. 7464).

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

12 (6) FEDERAL CYBERSECURITY ENHANCEMENT  
13 ACT OF 2015 UPDATE.—Section 222(3)(B) of the  
14 Federal Cybersecurity Enhancement Act of 2015 (6  
15 U.S.C. 1521(3)(B)) is amended by inserting “and  
16 the Committee on Oversight and Accountability” be-  
17 fore “of the House of Representatives”.

18 (j) FEDERAL CHIEF INFORMATION SECURITY OFFI-  
19 CER.—

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

1 **“§ 3617. Federal Chief Information Security Officer**

2 “(a) ESTABLISHMENT.—There is established a Fed-  
3 eral Chief Information Security Officer, who shall serve  
4 in—

5 “(1) the Office of the Federal Chief Informa-  
6 tion Officer of the Office of Management and Budg-  
7 et; and

8 “(2) the Office of the National Cyber Director.

9 “(b) APPOINTMENT.—The Federal Chief Information  
10 Security Officer shall be appointed by the President.

11 “(c) OMB DUTIES.—The Federal Chief Information  
12 Security Officer shall report to the Federal Chief Informa-  
13 tion Officer and assist the Federal Chief Information Offi-  
14 cer in carrying out—

15 “(1) every function under this chapter;

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

19 “(3) other electronic government initiatives con-  
20 sistent with other statutes; and

21 “(4) other Federal cybersecurity initiatives de-  
22 termined by the Federal Chief Information Officer.

23 “(d) ADDITIONAL DUTIES.—The Federal Chief In-  
24 formation Security Officer shall—

25 “(1) support the Federal Chief Information Of-  
26 ficer in overseeing and implementing Federal cyber-

1 security under the E–Government Act of 2002 (Pub-  
2 lic Law 107–347; 116 Stat. 2899) and other rel-  
3 evant statutes in a manner consistent with law; and

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

7 “(e) COORDINATION WITH ONCD.—The Federal  
8 Chief Information Security Officer shall support initiatives  
9 determined by the Federal Chief Information Officer nec-  
10 essary to coordinate with the Office of the National Cyber  
11 Director.”.

12 (2) NATIONAL CYBER DIRECTOR DUTIES.—Sec-  
13 tion 1752 of the William M. (Mac) Thornberry Na-  
14 tional Defense Authorization Act for Fiscal Year  
15 2021 (6 U.S.C. 1500) is amended—

16 (A) by redesignating subsection (g) as sub-  
17 section (h); and

18 (B) by inserting after subsection (f) the  
19 following:

20 “(g) SENIOR FEDERAL CYBERSECURITY OFFICER.—  
21 The Federal Chief Information Security Officer appointed  
22 by the President under section 3617 of title 44, United  
23 States Code, shall be a senior official within the Office  
24 and carry out duties applicable to the protection of infor-  
25 mation technology (as defined in section 11101 of title 40,

1 United States Code), including initiatives determined by  
2 the Director necessary to coordinate with the Office of the  
3 Federal Chief Information Officer.”.

4 (3) TREATMENT OF INCUMBENT.—The indi-  
5 vidual serving as the Federal Chief Information Se-  
6 curity Officer appointed by the President as of the  
7 date of enactment of this Act may serve as the Fed-  
8 eral Chief Information Security Officer under sec-  
9 tion 3617 of title 44, United States Code, as added  
10 by this section, beginning on the date of enactment  
11 of this section, without need for a further or addi-  
12 tional appointment under such section.

13 (4) CLERICAL AMENDMENT.—The table of sec-  
14 tions for chapter 36 of title 44, United States Code,  
15 is amended by adding at the end the following:

“3617. Federal Chief Information Security Officer.”.

16 (k) RENAMING OFFICE OF THE FEDERAL CHIEF IN-  
17 FORMATION OFFICER.—

18 (1) DEFINITIONS.—

19 (A) IN GENERAL.—Section 3601 of title  
20 44, United States Code, is amended—

21 (i) by striking paragraph (1); and

22 (ii) by redesignating paragraphs (2)  
23 through (8) as paragraphs (1) through (7),  
24 respectively.

25 (B) CONFORMING AMENDMENTS.—

1 (i) TITLE 10.—Section 2222(i)(6) of  
2 title 10, United States Code, is amended  
3 by striking “section 3601(4)” and insert-  
4 ing “section 3601”.

5 (ii) NATIONAL SECURITY ACT OF  
6 1947.—Section 506D(k)(1) of the National  
7 Security Act of 1947 (50 U.S.C.  
8 3100(k)(1)) is amended by striking “sec-  
9 tion 3601(4)” and inserting “section  
10 3601”.

11 (2) OFFICE OF ELECTRONIC GOVERNMENT.—  
12 Section 3602 of title 44, United States Code, is  
13 amended—

14 (A) in the heading, by striking “**Office of**  
15 **Electronic Government**” and inserting  
16 “**Office of the Federal Chief Informa-**  
17 **tion Officer**”;

18 (B) in subsection (a), by striking “Office  
19 of Electronic Government” and inserting “Of-  
20 fice of the Federal Chief Information Officer”;

21 (C) in subsection (b), by striking “an Ad-  
22 ministrator” and inserting “a Federal Chief In-  
23 formation Officer”;

24 (D) in subsection (c), in the matter pre-  
25 ceding paragraph (1), by striking “The Admin-

1           istrator” and inserting “The Federal Chief In-  
2           formation Officer”;

3           (E) in subsection (d), in the matter pre-  
4           ceding paragraph (1), by striking “The Admin-  
5           istrator” and inserting “The Federal Chief In-  
6           formation Officer”;

7           (F) in subsection (e), in the matter pre-  
8           ceding paragraph (1), by striking “The Admin-  
9           istrator” and inserting “The Federal Chief In-  
10          formation Officer”;

11          (G) in subsection (f)—

12           (i) in the matter preceding paragraph  
13           (1), by striking “the Administrator” and  
14           inserting “the Federal Chief Information  
15           Officer”;

16           (ii) in paragraph (16), by striking  
17           “the Office of Electronic Government” and  
18           inserting “the Office of the Federal Chief  
19           Information Officer”; and

20           (iii) in paragraph (17), by striking  
21           “E-Government” and inserting “annual”;  
22           and

23           (H) in subsection (g), by striking “the Of-  
24           fice of Electronic Government” and inserting

1 “the Office of the Federal Chief Information  
2 Officer”.

3 (3) CHIEF INFORMATION OFFICERS COUNCIL.—  
4 Section 3603 of title 44, United States Code, is  
5 amended—

6 (A) in subsection (b)(2), by striking “The  
7 Administrator of the Office of Electronic Gov-  
8 ernment” and inserting “The Federal Chief In-  
9 formation Officer”;

10 (B) in subsection (c)(1), by striking “The  
11 Administrator of the Office of Electronic Gov-  
12 ernment” and inserting “The Federal Chief In-  
13 formation Officer”; and

14 (C) in subsection (f)—

15 (i) in paragraph (3), by striking “the  
16 Administrator” and inserting “the Federal  
17 Chief Information Officer”; and

18 (ii) in paragraph (5), by striking “the  
19 Administrator” and inserting “the Federal  
20 Chief Information Officer”.

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

23 (A) in subsection (a)(2), by striking “the  
24 Administrator of the Office of Electronic Gov-



1           ernment” and inserting “the Federal Chief In-  
2           formation Officer”;

3           (B) in subsection (b), by striking “Admin-  
4           istrator” each place it appears and inserting  
5           “Federal Chief Information Officer”; and

6           (C) in subsection (c), in the matter pre-  
7           ceding paragraph (1), by striking “the Adminis-  
8           trator” and inserting “the Federal Chief Infor-  
9           mation Officer”.

10          (5) PROGRAM TO ENCOURAGE INNOVATIVE SO-  
11          LUTIONS TO ENHANCE ELECTRONIC GOVERNMENT  
12          SERVICES AND PROCESSES.—Section 3605 of title  
13          44, United States Code, is amended—

14               (A) in subsection (a), by striking “The Ad-  
15               ministrator” and inserting “The Federal Chief  
16               Information Officer”;

17               (B) in subsection (b), by striking “, the  
18               Administrator,” and inserting “, the Federal  
19               Chief Information Officer,”; and

20               (C) in subsection (c)(1)—

21                       (i) by striking “The Administrator”  
22                       and inserting “The Federal Chief Informa-  
23                       tion Officer”; and

24                       (ii) by striking “proposals submitted  
25                       to the Administrator” and inserting “pro-

1 posals submitted to the Federal Chief In-  
2 formation Officer”;

3 (D) in subsection (c)(2)(B), by striking  
4 “the Administrator” and inserting “the Federal  
5 Chief Information Officer”; and

6 (E) in subsection (c)(4), by striking “the  
7 Administrator” and inserting “the Federal  
8 Chief Information Officer”.

9 (6) E-GOVERNMENT REPORT.—Section 3606 of  
10 title 44, United States Code, is amended—

11 (A) in the section heading by striking “**E-**  
12 **Government**” and inserting “**Annual**”;

13 (B) in subsection (a), by striking “E-Gov-  
14 ernment” and inserting “annual”; and

15 (C) in subsection (b)(1), by striking  
16 “202(f)” and inserting “202(g)”.

17 (7) TREATMENT OF INCUMBENT.—The indi-  
18 vidual serving as the Administrator of the Office of  
19 Electronic Government under section 3602 of title  
20 44, United States Code, as of the date of enactment  
21 of this Act, may continue to serve as the Federal  
22 Chief Information Officer commencing as of that  
23 date, without need for a further or additional ap-  
24 pointment under such section.

1           (8) TECHNICAL AND CONFORMING AMEND-  
2           MENTS.—The table of sections for chapter 36 of title  
3           44, United States Code, is amended—

4                   (A) by striking the item relating to section  
5           3602 and inserting the following:

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

6           and

7                   (B) in the item relating to section 3606, by  
8           striking “E–Government” and inserting “An-  
9           nual”.

10          (9) REFERENCES.—

11                   (A) ADMINISTRATOR.—Any reference to  
12           the Administrator of the Office of Electronic  
13           Government in any law, regulation, map, docu-  
14           ment, record, or other paper of the United  
15           States shall be deemed to be a reference to the  
16           Federal Chief Information Officer.

17                   (B) OFFICE OF ELECTRONIC GOVERN-  
18           MENT.—Any reference to the Office of Elec-  
19           tronic Government in any law, regulation, map,  
20           document, record, or other paper of the United  
21           States shall be deemed to be a reference to the  
22           Office of the Federal Chief Information Officer.

23          (1) RULES OF CONSTRUCTION.—

24                   (1) AGENCY ACTIONS.—Nothing in this section,  
25           or an amendment made by this section, shall be con-

1       strued to authorize the head of an agency to take an  
2       action that is not authorized by this section, an  
3       amendment made by this section, or existing law.

4           (2) PROTECTION OF RIGHTS.—Nothing in this  
5       section, or an amendment made by this section, shall  
6       be construed to permit the violation of the rights of  
7       any individual protected by the Constitution of the  
8       United States, including through censorship of  
9       speech protected by the Constitution of the United  
10      States or unauthorized surveillance.

11          (3) PROTECTION OF PRIVACY.—Nothing in this  
12      section, or an amendment made by this section, shall  
13      be construed to—

14           (A) impinge on the privacy rights of indi-  
15      viduals; or

16           (B) allow the unauthorized access, sharing,  
17      or use of personal data.

18      (m) DEFINITIONS.—In t his section, unless otherwise  
19      specified:

20           (1) The term “agency” has the meaning given  
21      the term in section 3502 of title 44, United States  
22      Code.

23           (2) The term “appropriate congressional com-  
24      mittees” means—

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

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

14 (5) The term “Director” means the Director of  
15 the Office of Management and Budget.

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

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

22 (8) The term “national security system” has  
23 the meaning given the term in section 3552(b) of  
24 title 44, United States Code.

1           (9) The term “penetration test” has the mean-  
2           ing given the term in section 3552(b) of title 44,  
3           United States Code, as amended by this section.

4           (10) The term “threat hunting” means  
5           proactively and iteratively searching systems for  
6           threats and vulnerabilities, including threats or  
7           vulnerabilities that may evade detection by auto-  
8           mated threat detection systems.

9           (11) The term “zero trust architecture” has the  
10          meaning given the term in Special Publication 800-  
11          207 of the National Institute of Standards and  
12          Technology, or any successor document.

