

**AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 6497  
OFFERED BY MRS. CAROLYN B. MALONEY OF  
NEW YORK**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Federal Information  
3 Security Modernization Act of 2022”.

**4 SEC. 2. TABLE OF CONTENTS.**

5 The table of contents for this Act is as follows:

- Sec. 1. Short title.
- Sec. 2. Table of contents.
- Sec. 3. Definitions.

**TITLE I—UPDATES TO FISMA**

- Sec. 101. Title 44 amendments.
- Sec. 102. Amendments to subtitle III of title 40.
- Sec. 103. Actions to enhance Federal incident response.
- Sec. 104. Additional guidance to agencies on FISMA updates.
- Sec. 105. Agency requirements to notify private sector entities impacted by incidents.

**TITLE II—IMPROVING FEDERAL CYBERSECURITY**

- Sec. 201. Mobile security standards.
- Sec. 202. Data and logging retention for incident response.
- Sec. 203. Federal penetration testing policy.
- Sec. 204. Ongoing threat hunting program.
- Sec. 205. Vulnerability disclosure programs.
- Sec. 206. Implementing zero trust architecture.
- Sec. 207. GAO automation report.
- Sec. 208. Extension of Federal Acquisition Security Council.
- Sec. 209. Renaming of Office of the Federal Chief Information Officer.
- Sec. 210. Federal Chief Information Security Officer.
- Sec. 211. Extension of Chief Data Officer Council.

- Sec. 212. Council of the inspectors general on integrity and efficiency dashboard.
- Sec. 213. Quantitative cybersecurity metrics.

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL  
CYBERSECURITY

- Sec. 301. Risk-based budget pilot.
- Sec. 302. Active cyber defensive study.
- Sec. 303. Security operations center as a service pilot.
- Sec. 304. Detection and response as a service pilot.

**1 SEC. 3. DEFINITIONS.**

2 In this Act, unless otherwise specified:

3 (1) ADDITIONAL CYBERSECURITY PROCE-  
4 DURE.—The term “additional cybersecurity proce-  
5 dure” has the meaning given the term in section  
6 3552(b) of title 44, United States Code, as amended  
7 by this Act.

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

11 (3) APPROPRIATE CONGRESSIONAL COMMIT-  
12 TEES.—The term “appropriate congressional com-  
13 mittees” means—

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

16 (B) the Committee on Oversight and Re-  
17 form of the House of Representatives; and

18 (C) the Committee on Homeland Security  
19 of the House of Representatives.

1           (4) DIRECTOR.—The term “Director” means  
2           the Director of the Office of Management and Budg-  
3           et.

4           (5) INCIDENT.—The term “incident” has the  
5           meaning given the term in section 3552(b) of title  
6           44, United States Code.

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

11          (7) PENETRATION TEST.—The term “penetra-  
12          tion test” has the meaning given the term in section  
13          3552(b) of title 44, United States Code, as amended  
14          by this Act.

15          (8) THREAT HUNTING.—The term “threat  
16          hunting” means iteratively searching systems for  
17          threats and vulnerabilities that evade automated  
18          threat detection systems.

19          (9) ZERO TRUST ARCHITECTURE.—The term  
20          “zero trust architecture” means a security model, a  
21          set of system design principles, and a coordinated  
22          cybersecurity and system management strategy that  
23          employs continuous monitoring, risk-based access  
24          controls, or system security automation techniques  
25          to address the cybersecurity principle that threats

1 exist both inside and outside traditional network  
2 boundaries with an assumption that an incident is  
3 inevitable or has likely already occurred, and there-  
4 fore employs least-privileged access for network or  
5 system users while monitoring for anomalous or ma-  
6 licious activity.

## 7 **TITLE I—UPDATES TO FISMA**

### 8 **SEC. 101. TITLE 44 AMENDMENTS.**

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

11 (1) in subsection (a)(1)(B) of section 3504—

12 (A) by striking clause (v) and inserting the  
13 following:

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

16 (B) by redesignating clause (vi) as clause  
17 (vii); and

18 (C) by inserting after clause (v) the fol-  
19 lowing:

20 “(vi) in consultation with the National  
21 Cyber Director, confidentiality and security  
22 of information; and”;

23 (2) in section 3505—

24 (A) in paragraph (2) of the first subsection  
25 designated as subsection (c) by adding “dis-

1           covery of internet-accessible information sys-  
2           tems and assets, as well as” after “an inventory  
3           under this subsection shall include”;

4                   (B) in paragraph (3) of the first subsection  
5           designated as subsection (c)—

6                           (i) in subparagraph (B)—

7                                   (I) by inserting “the Secretary of  
8                                   Homeland Security acting through the  
9                                   Director of the Cybersecurity and In-  
10                                  frastructure Security Agency, the Na-  
11                                  tional Cyber Director, and” before  
12                                  “the Comptroller General”; and

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

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

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

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

23                                  (C) by striking the second subsection des-  
24                                  ignated as subsection (c);

25                                  (3) in section 3506—

1 (A) in subsection (a)(3), by inserting “In  
2 carrying out these duties, the Chief Information  
3 Officer shall coordinate, as appropriate, with  
4 the Chief Data Officer in accordance with the  
5 designated functions under section 3520(e).”  
6 after “reduction of information collection bur-  
7 dens on the public.”;

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

10 (C) in subsection (g)—

11 (i) in paragraph (1) by striking “and”  
12 at the end;

13 (ii) in paragraph (2) by striking the  
14 period at the end and inserting “; and”;  
15 and

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

18 “(3)(A) Notwithstanding subsection (a)(2), the  
19 head of each agency (as that term is defined in sec-  
20 tion 901(b) of title 31, United States Code) shall  
21 designate a Chief Privacy Officer to carry out the  
22 privacy responsibilities of the agency under this sub-  
23 chapter. The Chief Privacy Officer shall serve in a  
24 central leadership position at the agency, have visi-  
25 bility into relevant agency operations, and be posi-

1           tioned highly enough within the agency to regularly  
2           engage with other agency leadership, including the  
3           head of the agency.

4           “(B) In an agency that has a privacy officer  
5           created by another statute, such officer may carry  
6           out the responsibilities identified in subparagraph  
7           (A).”; and

8           (4) in section 3513—

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

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

13          “(c) Each agency providing a written plan under sub-  
14          section (b) shall provide any portion of the written plan  
15          addressing information security to the National Cyber Di-  
16          rector.”.

17          (b) SUBCHAPTER II DEFINITIONS.—

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

20                  (A) by redesignating paragraphs (1), (2),  
21                  (3), (4), (5), (6), and (7) as paragraphs (2),  
22                  (4), (5), (6), (7), (9), and (11), respectively;

23                  (B) by inserting before paragraph (2), as  
24                  so redesignated, the following:

1           “(1) The term ‘additional cybersecurity proce-  
2           dure’ means a process, procedure, or other activity  
3           that is established in excess of the information secu-  
4           rity standards promulgated under section 11331(b)  
5           of title 40 to increase the security and reduce the cy-  
6           bersecurity risk of agency systems.”;

7           (C) by inserting after paragraph (2), as so  
8           redesignated, the following:

9           “(3) The term ‘high value asset’ means infor-  
10          mation or an information system that the head of an  
11          agency determines, using policies, principles, stand-  
12          ards, or guidelines issued by the Director under sec-  
13          tion 3553(a), to be so critical to the agency that the  
14          loss or corruption of the information or the loss of  
15          access to the information system would have a seri-  
16          ous impact on the ability of the agency to perform  
17          the mission of the agency or conduct business.”;

18          (D) by inserting after paragraph (7), as so  
19          redesignated, the following:

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

23          (E) by inserting after paragraph (9), as so  
24          redesignated, the following:



1           “(10) The term ‘penetration test’ has the mean-  
2           ing given the term in guidance issued by the Direc-  
3           tor.”; and

4                   (F) by inserting after paragraph (11), as  
5           so redesignated, the following:

6           “(12) The term ‘shared service’ means a cen-  
7           tralized business or mission capability that is pro-  
8           vided to multiple organizations within an agency or  
9           to multiple agencies.”.

10           (2) CONFORMING AMENDMENTS.—

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

16                   (B) TITLE 10.—

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

21                           (ii) SECTION 2223.—Section  
22           2223(c)(3) of title 10, United States Code,  
23           is amended by striking “section  
24           3552(b)(6)” and inserting “section  
25           3552(b)”.

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

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

10 (C) HIGH-PERFORMANCE COMPUTING ACT  
11 OF 1991.—Section 207(a) of the High-Perform-  
12 ance Computing Act of 1991 (15 U.S.C.  
13 5527(a)) is amended by striking “section  
14 3552(b)(6)(A)(i)” and inserting “section  
15 3552(b)(9)(A)(i)”.

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

22 (E) NATIONAL DEFENSE AUTHORIZATION  
23 ACT FOR FISCAL YEAR 2013.—Section  
24 933(e)(1)(B) of the National Defense Author-  
25 ization Act for Fiscal Year 2013 (10 U.S.C.

1           2224 note) is amended by striking “section  
2           3542(b)(2)” and inserting “section 3552(b)”.

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

8                   (i) in section 806(e)(5) (10 U.S.C.  
9                   2304 note), by striking “section 3542(b)”  
10                  and inserting “section 3552(b)”;

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

15                   (iii) in section 932(b)(2) (10 U.S.C.  
16                   2224 note), by striking “section  
17                   3542(b)(2)” and inserting “section  
18                   3552(b)”.

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

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

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

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

6                   (ii) in subsection (f)—

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

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

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

16                   (1) in section 3551—

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

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

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

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

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

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

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

13           (2) in section 3553—

14           (A) in subsection (a)—

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

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

19           and

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

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

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

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

7               “(B) the use of zero trust architecture to  
8       improve resiliency and timely response actions  
9       to incidents on Federal systems.”;

10              (B) in subsection (b)—

11              (i) in the matter preceding paragraph  
12              (1), by striking “The Secretary, in con-  
13              sultation with the Director” and inserting  
14              “‘The Secretary of Homeland Security, act-  
15              ing through the Director of the Cybersecu-  
16              rity and Infrastructure Security Agency  
17              and in consultation with the Director and  
18              the National Cyber Director’”;

19              (ii) in paragraph (2)(A), by inserting  
20              “and reporting requirements under sub-  
21              chapter IV of this chapter” after “section  
22              3556”;

23              (iii) redesignate paragraphs (8) and  
24              (9) as paragraphs (9) and (10), respec-  
25              tively; and

1 (iv) by inserting after paragraph (7),  
2 the following new paragraph:

3 “(8) expeditiously seek opportunities to reduce  
4 costs, administrative burdens, and other barriers to  
5 information technology security and modernization  
6 for Federal agencies, including through—

7 “(A) shared services for cybersecurity ca-  
8 pabilities identified as optimal by the Director,  
9 in coordination with the Secretary acting  
10 through the Director of the Cybersecurity and  
11 Infrastructure Security Agency and other agen-  
12 cies as appropriate; and

13 “(B) offering technical assistance and ex-  
14 pertise to agencies on the selection and success-  
15 ful engagement of highly adaptive cybersecurity  
16 service contracts and other relevant contracts  
17 provided by the U.S. General Services Adminis-  
18 tration;”;

19 (C) in subsection (c)—

20 (i) in the matter preceding paragraph  
21 (1), by striking “each year” and inserting  
22 “each year during which agencies are re-  
23 quired to submit reports under section  
24 3554(c)” and by striking “preceding year”  
25 and inserting “preceding two years”;

- 1 (ii) by striking paragraph (1);
- 2 (iii) by redesignating paragraphs (2),
- 3 (3), and (4) as paragraphs (1), (2), and
- 4 (3), respectively;
- 5 (iv) in paragraph (3), as so redesign-
- 6 nated, by striking “and” at the end; and
- 7 (v) by inserting after paragraph (3),
- 8 as so redesignated, the following:
- 9 “(4) a summary of each assessment of Federal
- 10 risk posture performed under subsection (i); and”;
- 11 (D) by redesignating subsections (i), (j),
- 12 (k), and (l) as subsections (j), (k), (l), and (m)
- 13 respectively;
- 14 (E) in subsection (h)—
- 15 (i) in paragraph (2)(A), by inserting
- 16 “and the National Cyber Director” after
- 17 “in coordination with the Director”;
- 18 (ii) in paragraph (2)(D), by inserting
- 19 “, the National Cyber Director,” after “no-
- 20 tify the Director”; and
- 21 (iii) in paragraph (3)(A)(iv), by in-
- 22 sserting “, the National Cyber Director,”
- 23 after “the Secretary provides prior notice
- 24 to the Director”;



1 (F) by inserting after subsection (h) the  
2 following:

3 “(i) FEDERAL RISK ASSESSMENTS.—On an ongoing  
4 and continuous basis, the Director of the Cybersecurity  
5 and Infrastructure Security Agency shall perform assess-  
6 ments using any available information on the cybersecu-  
7 rity posture of agencies, and brief the Director and Na-  
8 tional Cyber Director on the findings of those assessments  
9 including—

10 “(1) the status of agency cybersecurity remedial  
11 actions described in section 3554(b)(7);

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

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

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

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

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

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

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

3           “(9) agency system risk assessments performed  
4 under section 3554(a)(1)(A); and

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

8           (G) in subsection (j), as so redesignated—

9                   (i) by striking “Not later than” and  
10 inserting:

11           “(1) IN GENERAL.—Not later than”;

12                   (ii) by striking “regarding the spe-  
13 cific” and inserting “that includes a sum-  
14 mary of—

15                   “(A) the specific”;

16                   (iii) in paragraph (1)(A), as so des-  
17 igned, by striking the period at the end  
18 and inserting “; and”; and

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

21           “(B) the trends identified in the Federal  
22 risk assessments performed under subsection  
23 (i).

1           “(2) FORM.—The report required under para-  
2           graph (1) shall be unclassified but may include a  
3           classified annex.”; and

4                       (H) by adding at the end the following:

5           “(n) BINDING OPERATIONAL DIRECTIVES.—If the  
6           Director of the Cybersecurity and Infrastructure Security  
7           Agency issues a binding operational directive or an emer-  
8           gency directive under this section, not later than 7 days  
9           after the date on which the binding operational directive  
10          requires an agency to take an action, the Director of the  
11          Cybersecurity and Infrastructure Security Agency shall  
12          provide to the Director and National Cyber Director the  
13          status of the implementation of the binding operational  
14          directive at the agency.”;

15                       (3) in section 3554—

16                               (A) in subsection (a)—

17                                       (i) in paragraph (1)—

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

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

1           “(A) on an ongoing and continuous basis,  
2 performing an agency system risk assessment  
3 that—

4           “(i) identifies and documents the high  
5 value assets of the agency using guidance  
6 from the Director;

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

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

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

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

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

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

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

8                   “(IV) incidents; and

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

12                  “(vi) assesses the impacts of potential  
13                  agency incidents to agency systems, data,  
14                  and operations based on the evaluations  
15                  described in clauses (ii) and (iv) and the  
16                  agency systems identified under clause  
17                  (iii); and

18                  “(vii) assesses the consequences of po-  
19                  tential incidents occurring on agency sys-  
20                  tems that would impact systems at other  
21                  agencies, including due to interconnectivity  
22                  between different agency systems or oper-  
23                  ational reliance on the operations of the  
24                  system or data in the system;”;

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

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

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

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

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

17 “(E) providing an update on the ongoing  
18 and continuous assessment performed under  
19 subparagraph (A)—

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

23 “(ii) on a periodic basis, as deter-  
24 mined by guidance issued by the Director

1 but not less frequently than every 2 years,  
2 to—

3 “(I) the Director;

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

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

9 “(F) in consultation with the Director of  
10 the Cybersecurity and Infrastructure Security  
11 Agency and not less frequently than once every  
12 3 years, performing an evaluation of whether  
13 additional cybersecurity procedures are appro-  
14 priate for securing a system of, or under the  
15 supervision of, the agency, which shall—

16 “(i) be completed considering the  
17 agency system risk assessment performed  
18 under subparagraph (A); and

19 “(ii) include a specific evaluation for  
20 high value assets;

21 “(G) not later than 30 days after com-  
22 pleting the evaluation performed under sub-  
23 paragraph (F), providing the evaluation and an  
24 implementation plan, if applicable, for using ad-

1           ditional cybersecurity procedures determined to  
2           be appropriate to—

3                   “(i) the Director of the Cybersecurity  
4                   and Infrastructure Security Agency;

5                   “(ii) the Director; and

6                   “(iii) the National Cyber Director;

7                   and

8                   “(H) if the head of the agency determines  
9                   there is need for additional cybersecurity proce-  
10                  dures, ensuring that those additional cybersecu-  
11                  rity procedures are reflected in the budget re-  
12                  quest of the agency;”;

13                   (ii) in paragraph (2)—

14                           (I) in subparagraph (A), by in-  
15                           serting “in accordance with the agen-  
16                           cy system risk assessment performed  
17                           under paragraph (1)(A)” after “infor-  
18                           mation systems”;

19                           (II) in subparagraph (B)—

20                                   (aa) by striking “in accord-  
21                                   ance with standards” and insert-  
22                                   ing “in accordance with—

23                                   “(i) standards”; and

24                                   (bb) by adding at the end  
25                                   the following:



1 “(ii) the evaluation performed under  
2 paragraph (1)(F); and

3 “(iii) the implementation plan de-  
4 scribed in paragraph (1)(G);”; and

5 (III) in subparagraph (D), by in-  
6 sserting “, through the use of penetra-  
7 tion testing, the vulnerability disclo-  
8 sure program established under sec-  
9 tion 3559B, and other means,” after  
10 “periodically”; and

11 (B) in subsection (b)—

12 (i) by striking paragraph (1) and in-  
13 sserting the following:

14 “(1) pursuant to subsection (a)(1)(A), per-  
15 forming ongoing and continuous agency system risk  
16 assessment, which may include using automated  
17 tools consistent with standards and guidelines pro-  
18 mulgated under section 11331 of title 40, as applica-  
19 ble;”;

20 (ii) in paragraph (2)(D)—

21 (I) by redesignating clauses (iii)  
22 and (iv) as clauses (iv) and (v), re-  
23 spectively;

24 (II) by inserting after clause (ii)  
25 the following:

1           “(iii) binding operational directives  
2           and emergency directives promulgated by  
3           the Director of the Cybersecurity and In-  
4           frastructure Security Agency under section  
5           3553;” and

6                       (III) in clause (iv), as so redesign-  
7                       nated, by striking “as determined by  
8                       the agency; and” and inserting “as  
9                       determined by the agency, considering  
10                      the agency risk assessment performed  
11                      under subsection (a)(1)(A).”;

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

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

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

20                     “(7) a process for providing the status of every  
21                     remedial action, as well as unremediated identified  
22                     system vulnerabilities, to the Director and the Direc-  
23                     tor of the Cybersecurity and Infrastructure Security  
24                     Agency, using automation and machine-readable  
25                     data to the greatest extent practicable;” and

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

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

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

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

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

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

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

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

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

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

24 (C) in subsection (c)—

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

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

5 “(1) BIENNIAL REPORT.—Not later than 2  
6 years after the date of the enactment of the Federal  
7 Information Security Modernization Act of 2022 and  
8 not less frequently than once every 2 years there-  
9 after, using the continuous and ongoing agency sys-  
10 tem risk assessment under subsection (a)(1)(A), the  
11 head of each agency shall submit to the Director,  
12 the Director of the Cybersecurity and Infrastructure  
13 Security Agency, the majority and minority leaders  
14 of the Senate, the Speaker and minority leader of  
15 the House of Representatives, the Committee on  
16 Homeland Security and Governmental Affairs of the  
17 Senate, the Committee on Oversight and Reform of  
18 the House of Representatives, the Committee on  
19 Homeland Security of the House of Representatives,  
20 the Committee on Commerce, Science, and Trans-  
21 portation of the Senate, the Committee on Science,  
22 Space, and Technology of the House of Representa-  
23 tives, the appropriate authorization and appropria-  
24 tions committees of Congress, the National Cyber

1 Director, and the Comptroller General of the United  
2 States a report that—

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

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

16 “(C) summarizes the evaluation and imple-  
17 mentation plans described in subparagraphs (F)  
18 and (G) of subsection (a)(1) and whether those  
19 evaluation and implementation plans call for  
20 the use of additional cybersecurity procedures  
21 determined to be appropriate by the agency;  
22 and

23 “(D) summarizes the status of remedial  
24 actions identified by inspector general of the  
25 agency, the Comptroller General of the United

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

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

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

8 “(B) may include a classified annex.

9 “(3) ACCESS TO INFORMATION.—The head of  
10 an agency shall ensure that, to the greatest extent  
11 practicable, information is included in the unclassi-  
12 fied form of the report submitted by the agency  
13 under paragraph (2)(A).

14 “(4) BRIEFINGS.—During each year during  
15 which a report is not required to be submitted under  
16 paragraph (1), the Director shall provide to the con-  
17 gressional committees described in paragraph (1) a  
18 briefing summarizing current cybersecurity posture  
19 of agencies.”; and

20 (iii) in paragraph (5), as so redesign-  
21 nated, by inserting “, including the report-  
22 ing procedures established under section  
23 11315(d) of title 40 and subsection  
24 (a)(3)(A)(v) of this section,” after “poli-  
25 cies, procedures, and practices”; and

1 (4) in section 3555—

2 (A) in the section heading, by striking  
3 “**ANNUAL INDEPENDENT**” and inserting  
4 “**INDEPENDENT**”;

5 (B) in subsection (a)—

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

10 (ii) in paragraph (2)(A), by inserting  
11 “, including by penetration testing and  
12 analyzing the vulnerability disclosure pro-  
13 gram of the agency” after “information  
14 systems”; and

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

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

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

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

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

3 “(f) PROTECTION OF INFORMATION.—(1) Agencies,  
4 evaluators, and other recipients of information that, if dis-  
5 closed, may cause harm to the efforts of Federal informa-  
6 tion security officers, shall take appropriate steps to en-  
7 sure the protection of that information, including safe-  
8 guarding the information from public disclosure.

9 “(2) The protections required under paragraph (1)  
10 shall be commensurate with the risk and comply with all  
11 applicable laws and regulations.

12 “(3) With respect to information that is not related  
13 to national security systems, agencies and evaluators shall  
14 make a summary of the information unclassified and pub-  
15 licly available, including information that does not iden-  
16 tify—

17 “(A) specific information system incidents; or

18 “(B) specific information system  
19 vulnerabilities.”;

20 (F) in subsection (g)(2)—

21 (i) by striking “this subsection shall”

22 and inserting “this subsection—

23 “(A) shall”;



1 (ii) in subparagraph (A), as so des-  
2 ignated, by striking the period at the end  
3 and inserting “; and”; and

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

6 “(B) identify any entity that performs an  
7 independent evaluation under subsection (b).”;  
8 and

9 (G) striking subsection (j); and  
10 (5) in section 3556(a)(4) by striking “3554(b)”  
11 and inserting “3554(a)(1)(A)”.

12 (d) CONFORMING AMENDMENTS.—

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

“3555. Independent evaluation.”.

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

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

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

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

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

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

15 (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

19 “SUBCHAPTER IV—FEDERAL SYSTEM  
20 INCIDENT RESPONSE

21 “§ 3591. Definitions

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

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

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

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

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

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

11           “(D) the Committee on Oversight and Re-  
12 form of the House of Representatives;

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

15           “(F) the appropriate authorization and ap-  
16 propriations committees of Congress;

17           “(G) the Director;

18           “(H) the Director of the Cybersecurity and  
19 Infrastructure Security Agency;

20           “(I) the National Cyber Director;

21           “(J) the Comptroller General of the United  
22 States; and

23           “(K) the inspector general of any impacted  
24 agency.

25           “(2) AWARDEE.—The term ‘awardee’—

1           “(A) means a person, business, or other  
2           entity that receives a grant from, or is a party  
3           to a cooperative agreement or an other trans-  
4           action agreement with, an agency; and

5           “(B) includes any subgrantee of a person,  
6           business, or other entity described in subpara-  
7           graph (A).

8           “(3) BREACH.—The term ‘breach’ shall be de-  
9           fined by the Director.

10          “(4) CONTRACTOR.—The term ‘contractor’  
11          means a prime contractor of an agency or a subcon-  
12          tractor of a prime contractor of an agency.

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

18          “(6) FEDERAL INFORMATION SYSTEM.—The  
19          term ‘Federal information system’ means an infor-  
20          mation system used or operated by an agency, a con-  
21          tractor, or another organization on behalf of an  
22          agency.

23          “(7) INTELLIGENCE COMMUNITY.—The term  
24          ‘intelligence community’ has the meaning given the

1 term in section 3 of the National Security Act of  
2 1947 (50 U.S.C. 3003).

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

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

11 **“§ 3592. Notification of breach**

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

18 “(1) determine whether notice to any individual  
19 potentially affected by the breach is appropriate  
20 based on an assessment of the risk of harm to the  
21 individual that considers—

22 “(A) the nature and sensitivity of the per-  
23 sonally identifiable information affected by the  
24 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) as appropriate, provide written notice in  
8           accordance with subsection (b) to each individual po-  
9           tentially affected by the breach—

10           “(A) to the last known mailing address of  
11           the individual; or

12           “(B) through an appropriate alternative  
13           method of notification that the head of the  
14           agency or a designated senior-level individual of  
15           the agency selects based on factors determined  
16           by the Director.

17           “(b) CONTENTS OF NOTICE.—Each notice of a  
18           breach provided to an individual under subsection (a)(2)  
19           shall include—

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

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

24           “(3) contact information of the agency that  
25           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 Federal law enforcement agencies and  
12          each nationwide consumer reporting agency; and

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

16          “(c) DELAY OF NOTIFICATION.—

17                 “(1) IN GENERAL.—The Attorney General, the  
18                 Director of National Intelligence, or the Secretary of  
19                 Homeland Security may delay a notification required  
20                 under subsection (a) if the notification would—

21                         “(A) impede a criminal investigation or a  
22                         national security activity;

23                         “(B) reveal sensitive sources and methods;

24                         “(C) cause damage to national security; or

25                         “(D) hamper security remediation actions.

1           “(2) DOCUMENTATION.—

2                   “(A) IN GENERAL.—Any delay under para-  
3 graph (1) shall be reported in writing to the Di-  
4 rector, the Attorney General, the Director of  
5 National Intelligence, the Secretary of Home-  
6 land Security, the National Cyber Director, the  
7 Director of the Cybersecurity and Infrastruc-  
8 ture Security Agency, and the head of the agen-  
9 cy and the inspector general of the agency that  
10 experienced the breach.

11                   “(B) CONTENTS.—A report required under  
12 subparagraph (A) shall include a written state-  
13 ment from the entity that delayed the notifica-  
14 tion explaining the need for the delay.

15                   “(C) FORM.—The report required under  
16 subparagraph (A) shall be unclassified but may  
17 include a classified annex.

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

20           “(d) UPDATE NOTIFICATION.—If an agency deter-  
21 mines there is a significant change in the reasonable basis  
22 to conclude that a breach occurred, a significant change  
23 to the determination made under subsection (a)(1), or that  
24 it is necessary to update the details of the information pro-  
25 vided to potentially affected individuals as described in



1 subsection (b), the agency shall as expeditiously as prac-  
2 ticable and without unreasonable delay, and in any case  
3 not later than 30 days after such a determination, notify  
4 each individual who received a notification pursuant to  
5 subsection (a) of those changes.

6 “(e) RULE OF CONSTRUCTION.—Nothing in this sec-  
7 tion shall be construed to limit—

8 “(1) the Director from issuing guidance relat-  
9 ing to notifications or the head of an agency from  
10 notifying individuals potentially affected by breaches  
11 that are not determined to be major incidents; or

12 “(2) the Director from issuing guidance relat-  
13 ing to notifications of major incidents or the head of  
14 an agency from providing more information than de-  
15 scribed in subsection (b) when notifying individuals  
16 potentially affected by breaches.

17 **“§ 3593. Congressional and executive branch reports**

18 “(a) INITIAL REPORT.—

19 “(1) IN GENERAL.—Not later than 72 hours  
20 after an agency has a reasonable basis to conclude  
21 that a major incident occurred, the head of the  
22 agency impacted by the major incident shall submit  
23 to the appropriate reporting entities a written re-  
24 port. Within 7 days of a major incident determina-  
25 tion, the head of the agency impacted, or their des-

1       ignee, shall coordinate with the National Cyber Di-  
2       rector, or their designee, to provide a briefing, along  
3       with the Director and any other Federal entity de-  
4       termined appropriate by the National Cyber Direc-  
5       tor, to the Committee on Homeland Security and  
6       Governmental Affairs of the Senate, the Committee  
7       on Oversight and Reform of the House of Represent-  
8       atives, the Committee on Homeland Security of the  
9       House of Representatives, and the appropriate au-  
10      thorization and appropriations committees of Con-  
11      gress, in the manner requested by the Congressional  
12      entities, taking into account—

13               “(A) the information known at the time of  
14               the report, including the threat having likely  
15               caused the major incident;

16               “(B) the sensitivity of the details associ-  
17               ated with the major incident; and

18               “(C) the classification level of the informa-  
19               tion contained in the report.

20               “(2) CONTENTS.—A report required under  
21               paragraph (1) shall include, in a manner that ex-  
22               cludes or otherwise reasonably protects personally  
23               identifiable information and to the extent permitted  
24               by applicable law, including privacy and statistical  
25               laws—

1           “(A) a summary of the information avail-  
2           able about the major incident, including how  
3           the major incident occurred and, if applicable,  
4           information relating to the major incident as a  
5           breach, based on information available to agen-  
6           cy officials as of the date on which the agency  
7           submits the report;

8           “(B) if applicable, whether any ransom has  
9           been demanded or paid, or plans to be paid, by  
10          any entity operating a Federal information sys-  
11          tem or with access to Federal information or a  
12          Federal information system, including the name  
13          of the entity demanding ransom, the date of the  
14          demand, and the amount and type of currency  
15          demanded, unless disclosure of such informa-  
16          tion will disrupt an active Federal law enforce-  
17          ment or national security operation;

18          “(C) if applicable, a description and any  
19          associated documentation of any circumstances  
20          necessitating a delay in notification to individ-  
21          uals potentially affected by the major incident  
22          under subsection (c) of section 3592; and

23          “(D) if applicable, an assessment of the  
24          impacts to the agency, the Federal Government,  
25          or the security of the United States, based on

1 information available to agency officials on the  
2 date on which the agency submits the report.

3 “(3) COMPONENTS OF BRIEFING.—The 7 day  
4 briefing required under paragraph (1)—

5 “(A) shall, to the greatest extent prac-  
6 ticable, include an unclassified component; and

7 “(B) may include a classified component.

8 “(b) SUPPLEMENTAL REPORT.—Within a reasonable  
9 amount of time, but not later than 30 days after the date  
10 on which an agency submits a written report under sub-  
11 section (a), the head of the agency shall provide to the  
12 appropriate reporting entities written updates on the  
13 major incident and, to the extent practicable, offer a brief-  
14 ing to the congressional committees described in sub-  
15 section (a)(1), including summaries of—

16 “(1) vulnerabilities, means by which the major  
17 incident occurred, and impacts to the agency relat-  
18 ing to the major incident;

19 “(2) any risk assessment and subsequent risk-  
20 based security implementation of the affected infor-  
21 mation system before the date on which the major  
22 incident occurred;

23 “(3) an estimate of the number of individuals  
24 potentially affected by the major incident based on

1 information available to agency officials as of the  
2 date on which the agency provides the update;

3 “(4) an assessment of the risk of harm to indi-  
4 viduals potentially affected by the major incident  
5 based on information available to agency officials as  
6 of the date on which the agency provides the update;

7 “(5) an update to the assessment of the risk to  
8 agency operations, or to impacts on other agency or  
9 non-Federal entity operations, affected by the major  
10 incident based on information available to agency of-  
11 ficials as of the date on which the agency provides  
12 the update; and

13 “(6) the detection, response, and remediation  
14 actions of the agency, including any support pro-  
15 vided by the Cybersecurity and Infrastructure Secu-  
16 rity Agency under section 3594(d) and status up-  
17 dates on the notification process described in section  
18 3592(a), including any delay described in subsection  
19 (c) of section 3592, if applicable.

20 “(c) UPDATE REPORT.—If the agency, the Director,  
21 or the National Cyber Director, determines that there is  
22 any significant change in the understanding of the agency  
23 of the scope, scale, or consequence of a major incident for  
24 which an agency submitted a written report under sub-  
25 section (a), the agency shall provide an updated report to

1 the appropriate reporting entities that includes informa-  
2 tion relating to the change in understanding.

3 “(d) BIENNIAL REPORT.—Each agency shall submit  
4 as part of the biannual report required under section  
5 3554(c)(1) of this title a description of each major inci-  
6 dent that occurred during the 2-year period preceding the  
7 date on which the biannual report is submitted.

8 “(e) DELAY REPORT.—

9 “(1) IN GENERAL.—The Director shall submit  
10 to the appropriate reporting entities an annual re-  
11 port on all notification delays granted pursuant to  
12 subsection (c) of section 3592.

13 “(2) COMPONENT OF OTHER REPORT.—The Di-  
14 rector may submit the report required under para-  
15 graph (1) as a component of the annual report sub-  
16 mitted under section 3597(b).

17 “(f) REPORT AND BRIEFING CONSISTENCY.—In car-  
18 rying out the duties under this section, and to achieve con-  
19 sistent and understandable agency reporting to Congress,  
20 the National Cyber Director, in coordination with the Di-  
21 rector, shall—

22 “(1) provide to agencies formatting guidelines  
23 and recommended contents of information to be in-  
24 cluded in the reports and briefings required under  
25 this section, including recommendations for the use

1 of plain language terminology and consistent for-  
2 mats for presenting any associated metrics; and

3 “(2) maintain a historical archive and major in-  
4 cident log of all reports and briefings provided under  
5 the requirements of this section, which shall include  
6 at a minimum an archive of the full contents of any  
7 written report and associated documentation, the re-  
8 porting agency, the date of submission, and a list of  
9 the recipient Congressional entities, which shall be  
10 made available upon request to the Congressional  
11 entities listed under subsection (a)(1).

12 “(g) REPORT DELIVERY.—Any written report re-  
13 quired to be submitted under this section may be sub-  
14 mitted in a paper or electronic format.

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

17 “(1) the ability of an agency to provide addi-  
18 tional reports or briefings to Congress; or

19 “(2) Congress from requesting additional infor-  
20 mation from agencies through reports, briefings, or  
21 other means.

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

24 “(a) IN GENERAL.—

1           “(1) INCIDENT REPORTING.—Subject to limita-  
2           tions in subsection (b), the head of each agency, or  
3           their designee, shall provide the information de-  
4           scribed in paragraph (2) relating to an incident af-  
5           fecting the agency, whether the information is ob-  
6           tained by the Federal Government directly or indi-  
7           rectly, to the Cybersecurity and Infrastructure Secu-  
8           rity Agency, the Office of Management and Budget,  
9           and the Office of the National Cyber Director in a  
10          manner specified by the Director under subsection  
11          (b).

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

15                 “(A) include detailed information about  
16                 the safeguards that were in place when the inci-  
17                 dent occurred;

18                 “(B) whether the agency implemented the  
19                 safeguards described in subparagraph (A) cor-  
20                 rectly;

21                 “(C) in order to protect against a similar  
22                 incident, identify—

23                         “(i) how the safeguards described in  
24                         subparagraph (A) should be implemented  
25                         differently; and



1 “(ii) additional necessary safeguards;

2 and

3 “(D) include information to aid in incident  
4 response, such as—

5 “(i) a description of the affected sys-  
6 tems or networks;

7 “(ii) the estimated dates of when the  
8 incident occurred; and

9 “(iii) information that could reason-  
10 ably help identify the party that conducted  
11 the incident, as appropriate.

12 “(3) INFORMATION SHARING.—To the greatest  
13 extent practicable, the Director of the Cybersecurity  
14 and Infrastructure Security Agency shall—

15 “(A) share information relating to an inci-  
16 dent with any agencies that may be impacted  
17 by the incident, or are potentially susceptible or  
18 similarly targeted, as well as with appropriate  
19 Federal law enforcement agencies to facilitate  
20 any necessary threat response activities as re-  
21 quested; and

22 “(B) coordinate, in consultation with the  
23 National Cyber Director, any necessary infor-  
24 mation sharing efforts related to a major inci-  
25 dent with the private sector.

1           “(4) NATIONAL SECURITY SYSTEMS.—Each  
2           agency operating or exercising control of a national  
3           security system shall share information about inci-  
4           dents that occur on national security systems with  
5           the Director of the Cybersecurity and Infrastructure  
6           Security Agency to the extent consistent with stand-  
7           ards and guidelines for national security systems  
8           issued in accordance with law and as directed by the  
9           President.

10          “(b) COMPLIANCE.—The information provided and  
11          method of reporting under subsection (a) shall take into  
12          account the level of classification of the information and  
13          any information sharing limitations and protections, such  
14          as limitations and protections relating to law enforcement,  
15          national security, privacy, statistical confidentiality, or  
16          other factors determined by the Director in order to imple-  
17          ment subsection (a)(1) in a manner that enables auto-  
18          mated and consistent reporting.

19          “(c) INCIDENT RESPONSE.—Each agency that has a  
20          reasonable basis to conclude that a major incident oc-  
21          curred involving Federal information in electronic medium  
22          or form, as defined by the Director and not involving a  
23          national security system, regardless of delays from notifi-  
24          cation granted for a major incident, shall coordinate with  
25          the Cybersecurity and Infrastructure Security Agency to

1 facilitate asset response activities and recommendations  
2 for mitigating future incidents, and with appropriate Fed-  
3 eral law enforcement agencies to facilitate threat response  
4 activities, consistent with relevant policies, principles,  
5 standards, and guidelines on information security.

6 **“§ 3595. Responsibilities of contractors and awardees**

7 “(a) REPORTING.—

8 “(1) IN GENERAL.—Unless otherwise specified  
9 in a contract, grant, cooperative agreement, or any  
10 other transaction agreement, any contractor or  
11 awardee of an agency shall report to both the agency  
12 and the Cybersecurity and Infrastructure Security  
13 Agency within the same amount of time such agency  
14 is required to report an incident, if the contractor or  
15 awardee has a reasonable basis to suspect or con-  
16 clude that—

17 “(A) an incident or breach has occurred  
18 with respect to Federal information collected,  
19 used, or maintained by the contractor or award-  
20 ee in connection with the contract, grant, coop-  
21 erative agreement, or other transaction agree-  
22 ment of the contractor or awardee;

23 “(B) an incident or breach has occurred  
24 with respect to a Federal information system  
25 used or operated by the contractor or awardee

1 in connection with the contract, grant, coopera-  
2 tive agreement, or other transaction agreement  
3 of the contractor or awardee;

4 “(C) a component of any Federal informa-  
5 tion system used or operated by the contractor  
6 or awardee in connection with the contract,  
7 grant, cooperative agreement, or other trans-  
8 action agreement of the contractor or awardee  
9 contains a security vulnerability, including a  
10 supply chain compromise or an identified soft-  
11 ware or hardware vulnerability; or

12 “(D) the contractor or awardee has re-  
13 ceived information from the agency that the  
14 contractor or awardee is not authorized to re-  
15 ceive in connection with the contract, grant, co-  
16 operative agreement, or other transaction agree-  
17 ment of the contractor or awardee.

18 “(2) PROCEDURES.—

19 “(A) MAJOR INCIDENT.—Following a re-  
20 port of a breach or major incident by a con-  
21 tractor or awardee under paragraph (1), the  
22 agency, in consultation with the contractor or  
23 awardee and as coordinated by the National  
24 Cyber Director, shall carry out the require-

1           ments under sections 3592, 3593, and 3594  
2           with respect to the breach or major incident.

3           “(B) INCIDENT.—Following a report of an  
4           incident by a contractor or awardee under para-  
5           graph (1), an agency, in consultation with the  
6           contractor or awardee and as coordinated by  
7           the National Cyber Director, shall carry out the  
8           requirements under section 3594 with respect  
9           to the incident.

10          “(b) EFFECTIVE DATE.—This section shall apply on  
11          and after the date that is 1 year after the date of the  
12          enactment of the Federal Information Security Mod-  
13          ernization Act of 2022 and shall apply with respect to any  
14          contract entered into on or after such effective date.

15          **“§ 3596. Training**

16          “(a) COVERED INDIVIDUAL DEFINED.—In this sec-  
17          tion, the term ‘covered individual’ means an individual  
18          who obtains access to Federal information or Federal in-  
19          formation systems because of the status of the individual  
20          as an employee, contractor, awardee, volunteer, or intern  
21          of an agency.

22          “(b) REQUIREMENT.—The head of each agency shall  
23          develop training for covered individuals on how to identify  
24          and respond to an incident, including—

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

3           “(2) the obligation of a covered individual to re-  
4           port to the agency a suspected major incident and  
5           any suspected incident involving information in any  
6           medium or form, including paper, oral, and elec-  
7           tronic.

8           “(c) INCLUSION IN ANNUAL TRAINING.—The train-  
9           ing developed under subsection (b) may be included as  
10          part of an annual privacy or security awareness training  
11          of an agency.

12       **“§ 3597. Analysis and report on Federal incidents**

13           “(a) ANALYSIS OF FEDERAL INCIDENTS.—

14           “(1) QUANTITATIVE AND QUALITATIVE ANAL-  
15           YSES.—The Director of the Cybersecurity and Infra-  
16           structure Security Agency shall develop, in consulta-  
17           tion with the Director and the National Cyber Direc-  
18           tor, and perform continuous monitoring and quan-  
19           titative and qualitative analyses of incidents at agen-  
20           cies, including major incidents, including—

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

22                           “(i) attacker tactics, techniques, and  
23                           procedures; and

24                           “(ii) system vulnerabilities, including  
25                           previously unknown zero day exploitations,

1           unpatched systems, and information sys-  
2           tem misconfigurations;

3           “(B) the scope and scale of incidents at  
4           agencies;

5           “(C) common root causes of incidents  
6           across multiple agencies;

7           “(D) agency incident response, recovery,  
8           and remediation actions and the effectiveness of  
9           those actions, as applicable;

10          “(E) lessons learned and recommendations  
11          in responding to, recovering from, remediating,  
12          and mitigating future incidents; and

13          “(F) trends across multiple Federal agen-  
14          cies to address intrusion detection and incident  
15          response capabilities using the metrics estab-  
16          lished under section 224(c) of the Cybersecurity  
17          Act of 2015 (6 U.S.C. 1522(c)).

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

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

23                 “(A) IN GENERAL.—The Director shall  
24                 share on an ongoing basis the analyses required

1 under this subsection with agencies and the Na-  
2 tional Cyber Director to—

3 “(i) improve the understanding of cy-  
4 bersecurity risk of agencies; and

5 “(ii) support the cybersecurity im-  
6 provement efforts of agencies.

7 “(B) FORMAT.—In carrying out subpara-  
8 graph (A), the Director shall share the anal-  
9 yses—

10 “(i) in human-readable written prod-  
11 ucts; and

12 “(ii) to the greatest extent practicable,  
13 in machine-readable formats in order to  
14 enable automated intake and use by agen-  
15 cies.

16 “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—  
17 Not later than 2 years after the date of the enactment  
18 of this section, and not less frequently than annually  
19 thereafter, the Director of the Cybersecurity and Infra-  
20 structure Security Agency, in consultation with the Direc-  
21 tor, the National Cyber Director, and the heads of other  
22 agencies as appropriate, shall submit to the appropriate  
23 reporting entities a report that includes—



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

4           “(2) the quantitative and qualitative analyses of  
5 incidents developed under subsection (a)(1) on an  
6 agency-by-agency basis and comprehensively across  
7 the Federal Government, including—

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

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

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

14                 “(A) a description of each major incident;  
15 and

16                 “(B) an analysis of the agency’s perform-  
17 ance against the metrics established under sec-  
18 tion 224(c) of the Cybersecurity Act of 2015 (6  
19 U.S.C. 1522(c)).

20           “(c) PUBLICATION.—To the extent that publication  
21 is consistent with national security interests, a summary  
22 report containing aggregated metrics and trends of the in-  
23 cident information contained in the reports submitted  
24 under subsection (b) shall be made publicly available on  
25 the website of the Cybersecurity and Infrastructure Secu-

1 rity Agency during the year in which the reports are sub-  
2 mitted.

3 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

8 “(2) NATIONAL SECURITY SYSTEM REPORTS.—

9 “(A) IN GENERAL.—Annually, the head of  
10 an agency that operates or exercises control of  
11 a national security system shall submit a report  
12 that includes the information described in sub-  
13 section (b) with respect to the agency to the ex-  
14 tent that the submission is consistent with  
15 standards and guidelines for national security  
16 systems issued in accordance with law and as  
17 directed by the President to—

18 “(i) the majority and minority leaders  
19 of the Senate,

20 “(ii) the Speaker and minority leader  
21 of the House of Representatives;

22 “(iii) the Committee on Homeland Se-  
23 curity and Governmental Affairs of the  
24 Senate;

1 “(iv) the Select Committee on Intel-  
2 ligence of the Senate;

3 “(v) the Committee on Armed Serv-  
4 ices of the Senate;

5 “(vi) the Committee on Appropria-  
6 tions of the Senate;

7 “(vii) the Committee on Oversight and  
8 Reform of the House of Representatives;

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

11 “(ix) the Permanent Select Committee  
12 on Intelligence of the House of Represent-  
13 atives;

14 “(x) the Committee on Armed Serv-  
15 ices of the House of Representatives; and

16 “(xi) the Committee on Appropria-  
17 tions of the House of Representatives.

18 “(B) CLASSIFIED FORM.—A report re-  
19 quired under subparagraph (A) may be sub-  
20 mitted in a classified form.

21 “(e) REQUIREMENT FOR COMPILING INFORMA-  
22 TION.—In publishing the public report required under  
23 subsection (c), the Director of the Cybersecurity and In-  
24 frastructure Security Agency shall sufficiently compile in-  
25 formation such that no specific incident of an agency can

1 be identified, except with the concurrence of the Director  
2 of the Office of Management and Budget, the National  
3 Cyber Director, and in consultation with the impacted  
4 agency.

5 **“§ 3598. Major incident definition**

6 “(a) IN GENERAL.—Not later than one year after the  
7 date of the enactment of the Federal Information Security  
8 Modernization Act of 2022, the Director, in coordination  
9 with the Director of the Cybersecurity and Infrastructure  
10 Security Agency and the National Cyber Director, shall  
11 develop and promulgate guidance on the definition of the  
12 term ‘major incident’ for the purposes of subchapter II  
13 and this subchapter.

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

17 “(1) include, with respect to any information  
18 collected or maintained by or on behalf of an agency  
19 or an information system used or operated by an  
20 agency or by a contractor of an agency or another  
21 organization on behalf of an agency, any incident  
22 the head of the agency determines with high con-  
23 fidence is likely to result in clear and demonstrable  
24 harm to—

1           “(A) the national security interests, foreign  
2 relations, or the economy of the United States;

3           “(B) the public confidence, civil liberties,  
4 or public health and safety of the people of the  
5 United States;

6           “(C) the privacy of the people of the  
7 United States, including the integrity of person-  
8 ally identifiable information; or

9           “(D) any other type of incident determined  
10 appropriate by the Director; and

11          “(2) stipulate that the National Cyber Director,  
12 in consultation with the Director, shall have the au-  
13 thority to declare a major incident, and in making  
14 such declaration shall consider whether an inci-  
15 dent—

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

17           “(B) is enabled by—

18           “(i) a common technical root cause,  
19 such as a supply chain compromise or a  
20 common software or hardware vulner-  
21 ability; or

22           “(ii) the related activities of a com-  
23 mon threat actor; or

1           “(C) has a significant impact on the con-  
2           fidentiality, integrity, or availability of a high  
3           value asset.

4           “(c) EVALUATION AND UPDATES.—Not later than 2  
5           years after the date on which the Director promulgates  
6           guidance as required in subsection (a), and not less fre-  
7           quently than every 2 years thereafter, the Director shall  
8           evaluate and update, if necessary, the guidance issued  
9           under subsection (a).”.

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

“SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

- “3591. Definitions.
- “3592. Notification of breach.
- “3593. Congressional and executive branch reports.
- “3594. Government information sharing and incident response.
- “3595. Responsibilities of contractors and awardees.
- “3596. Training.
- “3597. Analysis and report on Federal incidents.
- “3598. Major incident definition.”.

13 **SEC. 102. AMENDMENTS TO SUBTITLE III OF TITLE 40.**

14           (a) MODERNIZING GOVERNMENT TECHNOLOGY.—  
15           Subtitle G of title X of division A of the National Defense  
16           Authorization Act for Fiscal Year 2018 (Public Law 115–  
17           91; 40 U.S.C. 11301 note) is amended in section 1078—  
18           (1) by striking subsection (a) and inserting the  
19           following:

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

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

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

7           (2) in subsection (c)—

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

11                   (B) in paragraph (5)—

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

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

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

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

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

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

3 (1) in section 11302—

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

10 (B) by amending subsection (f) to read as  
11 follows:

12 “(f) USE OF BEST PRACTICES IN ACQUISITIONS.—  
13 The Director shall—

14 “(1) encourage the heads of the executive agen-  
15 cies to develop and use the best practices in the ac-  
16 quisition of information technology, including supply  
17 chain risk management standards, guidelines, and  
18 practices developed by the National Institute of  
19 Standards and Technology; and

20 “(2) consult with the Federal Chief Information  
21 Security Officer appointed by the President under  
22 section 3607 of title 44, for the development and use  
23 of risk management standards, guidelines, and prac-  
24 tices developed by the National Institute of Stand-  
25 ards and Technology.”; and



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

4 (2) in subparagraph (B) of section  
5 11303(b)(2)—

6 (A) in clause (i), by striking “; or” and in-  
7 serting a semicolon;

8 (B) in clause (ii), by striking the semicolon  
9 and inserting “; or” ; and

10 (C) by inserting at the end the following:

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

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

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

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

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

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

4 (d) SUBCHAPTER III.—Section 11331 of title 40,  
5 United States Code, is amended—

6 (1) in subsection (a), by striking “section  
7 3532(b)(1)” and inserting “section 3552(b)”;

8 (2) in subsection (b)(1)(A), by striking “the  
9 Secretary of Homeland Security” and inserting “the  
10 Director of the Cybersecurity and Infrastructure Se-  
11 curity Agency”;

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

13 “(e) REVIEW OF OFFICE OF MANAGEMENT AND  
14 BUDGET GUIDANCE AND POLICY.—

15 “(1) CONDUCT OF REVIEW.—The Director of  
16 the Office of Management and Budget shall regu-  
17 larly review the efficacy of the guidance and policy  
18 promulgated by the Director in reducing cybersecu-  
19 rity risks, including consideration of reporting and  
20 compliance burden on agencies.

21 “(2) GAO REVIEW.—The Government Account-  
22 ability Office shall regularly review the guidance and  
23 policy promulgated by the Director to assess its effi-  
24 cacy in risk reduction and burden on agencies, and  
25 shall issue recommendations to the Director.

1           “(f) 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) and (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, in consultation with the Director of the Cybersecu-  
10 rity and Infrastructure Security Agency, specifications to  
11 enable the automated verification of the implementation  
12 of controls.”.

13 **SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**  
14 **SPONSE.**

15           (a) RESPONSIBILITIES OF THE CYBERSECURITY AND  
16 INFRASTRUCTURE SECURITY AGENCY.—

17           (1) IN GENERAL.—Not later than 180 days  
18 after the date of the enactment of this Act, the Di-  
19 rector of the Cybersecurity and Infrastructure Secu-  
20 rity Agency shall—

21           (A) develop a plan for the development of  
22 the analysis required under section 3597(a) of  
23 title 44, United States Code, as added by this  
24 Act, and the report required under subsection

25           (b) of that section that includes—

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

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

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

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

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

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

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

23 (1) FISMA.—Section 2 of the Federal Informa-  
24 tion Security Modernization Act of 2014 (Public  
25 Law 113–283; 44 U.S.C. 3554 note) is amended—

1 (A) by striking subsection (b); and

2 (B) by redesignating subsections (c)  
3 through (f) as subsections (b) through (e), re-  
4 spectively.

5 (2) IN GENERAL.—The Director shall develop  
6 guidance, to be updated not less frequently than  
7 once every 2 years, on the content, timeliness, and  
8 format of the information provided by agencies  
9 under section 3594(a) of title 44, United States  
10 Code, as added by this Act.

11 (3) GUIDANCE ON RESPONDING TO INFORMA-  
12 TION REQUESTS.—Not later than 1 year after the  
13 date of the enactment of this Act, the Director shall  
14 develop guidance for agencies to implement the re-  
15 quirement under section 3594(c) of title 44, United  
16 States Code, as added by this Act, to provide infor-  
17 mation to other agencies experiencing incidents.

18 (4) STANDARD GUIDANCE AND TEMPLATES.—  
19 Not later than 1 year after the date of the enact-  
20 ment of this Act, the Director, in consultation with  
21 the Director of the Cybersecurity and Infrastructure  
22 Security Agency, shall develop guidance and, as ap-  
23 propriate, templates, to be reviewed and, if nec-  
24 essary, updated not less frequently than once every  
25 2 years, for use by agencies in the activities required

1 under sections 3592, 3593, and 3596 of title 44,  
2 United States Code, as added by this Act.

3 (5) CONTRACTOR AND AWARDEE GUIDANCE.—

4 (A) IN GENERAL.—Not later than 1 year  
5 after the date of the enactment of this Act, the  
6 Director, in coordination with the Secretary of  
7 Homeland Security, the Secretary of Defense,  
8 the Administrator of General Services, and the  
9 heads of other agencies determined appropriate  
10 by the Director, shall issue guidance to agencies  
11 on how to deconflict, to the greatest extent  
12 practicable, regulations, policies, and procedures  
13 relating to the responsibilities of contractors  
14 and awardees established under section 3595 of  
15 title 44, United States Code, as added by this  
16 Act.

17 (B) EXISTING PROCESSES.—To the great-  
18 est extent practicable, the guidance issued  
19 under subparagraph (A) shall allow contractors  
20 and awardees to use existing processes for noti-  
21 fying agencies of incidents involving information  
22 of the Federal Government.

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

1 (1) in paragraph (11), by striking “; or” and  
2 inserting a semicolon;

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

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

6 “(13) to another agency, to the extent nec-  
7 essary, in furtherance of a response to an incident  
8 (as defined in section 3552 of title 44) or to fulfill  
9 the information sharing requirements in section  
10 3594 of title 44, provided that the agency maintains  
11 a record specifying the particular portion desired  
12 and the activity for which the record is sought.”.

13 **SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**  
14 **UPDATES.**

15 Not later than 1 year after the date of the enactment  
16 of this Act, the Director shall issue guidance for agencies  
17 on—

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

22 (2) implementing additional cybersecurity pro-  
23 cedures, which shall include resources for shared  
24 services;

1           (3) establishing a process for providing the sta-  
2           tus of each remedial action under section 3554(b)(7)  
3           of title 44, United States Code, as amended by this  
4           Act, to the Director and the Director of the Cyberse-  
5           curity and Infrastructure Security Agency using au-  
6           tomation and machine-readable data, as practicable,  
7           which shall include—

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

10                   (B) templates for providing the status of  
11                   the remedial action;

12           (4) interpreting the definition of “high value  
13           asset” under section 3552 of title 44, United States  
14           Code, as amended by this Act; and

15           (5) a requirement to coordinate with inspectors  
16           general of agencies to ensure consistent under-  
17           standing and application of agency policies for the  
18           purpose of evaluations by inspectors general.

19 **SEC. 105. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**  
20 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

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

22           (1) **REPORTING ENTITY.**—The term “reporting  
23           entity” means a private organization or govern-  
24           mental unit that is required by statute or regulation  
25           to submit sensitive information to an agency.



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

5           (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-  
6           TITIES.—Not later than 180 days after the date of the  
7           enactment of this Act, the Director shall issue guidance  
8           requiring the head of each agency to notify a reporting  
9           entity of an incident that is likely to substantially affect—

10           (1) the confidentiality or integrity of sensitive  
11           information submitted by the reporting entity to the  
12           agency pursuant to a statutory or regulatory re-  
13           quirement; or

14           (2) each agency information system used in the  
15           transmission or storage of the sensitive information  
16           described in paragraph (1).

## 17       **TITLE II—IMPROVING FEDERAL** 18       **CYBERSECURITY**

### 19       **SEC. 201. MOBILE SECURITY STANDARDS.**

20           (a) IN GENERAL.—Not later than 1 year after the  
21           date of the enactment of this Act, the Director shall—

22           (1) evaluate mobile application security guid-  
23           ance promulgated by the Director; and

24           (2) issue guidance to secure mobile devices, in-  
25           cluding for mobile applications, for every agency.

1 (b) CONTENTS.—The guidance issued under sub-  
2 section (a)(2) shall include—

3 (1) a requirement, pursuant to section  
4 3506(b)(4) of title 44, United States Code, for every  
5 agency to maintain a continuous inventory of  
6 every—

7 (A) mobile device operated by or on behalf  
8 of the agency; and

9 (B) vulnerability identified by the agency  
10 associated with a mobile device; and

11 (2) a requirement for every agency to perform  
12 continuous evaluation of the vulnerabilities described  
13 in paragraph (1)(B) and other risks associated with  
14 the use of applications on mobile devices.

15 (c) INFORMATION SHARING.—The Director, in co-  
16 ordination with the Director of the Cybersecurity and In-  
17 frastructure Security Agency, shall issue guidance to  
18 agencies for sharing the inventory of the agency required  
19 under subsection (b)(1) with the Director of the Cyberse-  
20 curity and Infrastructure Security Agency, using automa-  
21 tion and machine-readable data to the greatest extent  
22 practicable.

23 (d) BRIEFING.—Not later than 60 days after the date  
24 on which the Director issues guidance under subsection  
25 (a)(2), the Director, in coordination with the Director of

1 the Cybersecurity and Infrastructure Security Agency,  
2 shall provide to the appropriate congressional committees  
3 a briefing on the guidance.

4 **SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT**  
5 **RESPONSE.**

6 (a) **RECOMMENDATIONS.**—Not later than 2 years  
7 after the date of the enactment of this Act, and not less  
8 frequently than every 2 years thereafter, the Director of  
9 the Cybersecurity and Infrastructure Security Agency, in  
10 consultation with the Attorney General, shall submit to  
11 the Director recommendations on requirements for logging  
12 events on agency systems and retaining other relevant  
13 data within the systems and networks of an agency.

14 (b) **CONTENTS.**—The recommendations provided  
15 under subsection (a) shall include—

- 16 (1) the types of logs to be maintained;
- 17 (2) the duration that logs and other relevant  
18 data should be retained;
- 19 (3) the time periods for agency implementation  
20 of recommended logging and security requirements;
- 21 (4) how to ensure the confidentiality, integrity,  
22 and availability of logs;
- 23 (5) requirements to ensure that, upon request,  
24 in a manner that excludes or otherwise reasonably  
25 protects personally identifiable information, and to

1 the extent permitted by applicable law (including  
2 privacy and statistical laws), agencies provide logs  
3 to—

4 (A) the Director of the Cybersecurity and  
5 Infrastructure Security Agency for a cybersecu-  
6 rity purpose; and

7 (B) the Director of the Federal Bureau of  
8 Investigation, or the appropriate Federal law  
9 enforcement agency, to investigate potential  
10 criminal activity; and

11 (6) requirements to ensure that, subject to com-  
12 pliance with statistical laws and other relevant data  
13 protection requirements, the highest level security  
14 operations center of each agency has visibility into  
15 all agency logs.

16 (c) GUIDANCE.—Not later than 90 days after receiv-  
17 ing the recommendations submitted under subsection (a),  
18 the Director, in consultation with National Cyber Direc-  
19 tor, the Director of the Cybersecurity and Infrastructure  
20 Security Agency, and the Attorney General, shall, as de-  
21 termined to be appropriate by the Director, update guid-  
22 ance to agencies regarding requirements for logging, log  
23 retention, log management, sharing of log data with other  
24 appropriate agencies, or any other logging activity deter-  
25 mined to be appropriate by the Director.

1 (d) SUNSET.—This section will cease to be in effect  
2 on the date that is 10 years after the date of the enact-  
3 ment of this Act.

4 **SEC. 203. FEDERAL PENETRATION TESTING POLICY.**

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

8 **“§ 3559A. Federal penetration testing**

9 “(a) GUIDANCE.—The Director shall, in consultation  
10 with the Secretary of Homeland Security acting through  
11 the Director of the Cybersecurity and Infrastructure Secu-  
12 rity Agency, issue guidance to agencies that—

13 “(1) requires agencies to use, when and where  
14 appropriate, penetration testing on agency systems  
15 by both Federal and non-Federal entities, with a  
16 focus on high value assets;

17 “(2) provides policies governing agency develop-  
18 ment of an operational plan, rules of engagement for  
19 utilizing penetration testing, and procedures to uti-  
20 lize the results of penetration testing to improve the  
21 cybersecurity and risk management of the agency;  
22 and

23 “(3) ensures that penetration testing is being  
24 performed appropriately by agencies and that oper-  
25 ational support or a shared service is available.

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

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

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

9                   “(2) to the Director of National Intelligence in  
10 the case of systems described in section  
11 3553(e)(3).”.

12           (b) DEADLINE FOR GUIDANCE.—Not later than 180  
13 days after the date of the enactment of this Act, the Direc-  
14 tor shall issue the guidance required under section  
15 3559A(a) of title 44, United States Code, as added by sub-  
16 section (a).

17           (c) SUNSET.—This section shall sunset and any  
18 amendments made by this section shall be repealed on the  
19 date that is 10 years after the date of the enactment of  
20 this Act.

21           (d) CLERICAL AMENDMENT.—The table of sections  
22 for chapter 35 of title 44, United States Code, is amended  
23 by adding after the item relating to section 3559 the fol-  
24 lowing:

“3559A. Federal penetration testing.”.

1 (e) PENETRATION TESTING BY THE SECRETARY OF  
2 HOMELAND SECURITY.—Section 3553(b) of title 44,  
3 United States Code, as amended by section 101, is further  
4 amended—

5 (1) by redesignating paragraphs (9) and (10)  
6 as paragraphs (10) and (11), respectively; and

7 (2) by inserting after paragraph (8) the fol-  
8 lowing:

9 “(9) performing penetration testing to identify  
10 vulnerabilities within Federal information systems;”.

11 **SEC. 204. ONGOING THREAT HUNTING PROGRAM.**

12 (a) THREAT HUNTING PROGRAM.—

13 (1) IN GENERAL.—Not later than 540 days  
14 after the date of the enactment of this Act, the Di-  
15 rector of the Cybersecurity and Infrastructure Secu-  
16 rity Agency shall establish a program to provide on-  
17 going threat-hunting services in accordance with au-  
18 thorities granted in section 3553(b)(9)–(10) and  
19 3553(m) of title 44, United States Code (as redesign-  
20 nated by this Act), and may offer such threat hunt-  
21 ing services as a shared service for the network of  
22 each agency.

23 (2) PLAN.—Not later than 180 days after the  
24 date of the enactment of this Act, the Director of  
25 the Cybersecurity and Infrastructure Security Agen-

1       cy shall develop a plan to establish the program re-  
2       quired under paragraph (1) that describes how the  
3       Director of the Cybersecurity and Infrastructure Se-  
4       curity Agency plans to—

5               (A) determine the method for collecting,  
6               storing, accessing, analyzing, and safeguarding  
7               appropriate agency data;

8               (B) provide on-premises support to agen-  
9               cies;

10              (C) staff threat hunting services;

11              (D) establish common operating proce-  
12              dures, including necessary interagency legal  
13              agreements;

14              (E) allocate available human and financial  
15              resources to implement the plan; and

16              (F) provide input to the heads of agencies  
17              on the use of—

18                      (i) more stringent standards under  
19                      section 11331(c)(1) of title 40, United  
20                      States Code; and

21                      (ii) additional cybersecurity proce-  
22                      dures under section 3554 of title 44,  
23                      United States Code.

24       (b) REPORTS.—The Director of the Cybersecurity  
25       and Infrastructure Security Agency, in consultation with



1 the Director, shall submit to the appropriate congressional  
2 committees—

3 (1) not later than 30 days after the date on  
4 which the Director of the Cybersecurity and Infra-  
5 structure Security Agency completes the plan re-  
6 quired under subsection (a)(2), a report on the plan  
7 to provide threat hunting services to agencies;

8 (2) not less than 30 days before the date on  
9 which the Director of the Cybersecurity and Infra-  
10 structure Security Agency begins providing threat  
11 hunting services under the program under sub-  
12 section (a)(1), a report providing any updates to the  
13 plan developed under subsection (a)(2); and

14 (3) not later than 1 year after the date on  
15 which the Director of the Cybersecurity and Infra-  
16 structure Security Agency begins providing threat  
17 hunting services to agencies other than the Cyberse-  
18 curity and Infrastructure Security Agency, a report  
19 describing lessons learned from providing those serv-  
20 ices.

21 **SEC. 205. VULNERABILITY DISCLOSURE PROGRAMS.**

22 (a) IN GENERAL.—Subchapter II of Chapter 35 of  
23 title 44, United States Code, as amended by section  
24 203(a), is further amended by adding at the end the fol-  
25 lowing:

1 **“§ 3559B. Federal vulnerability disclosure programs**

2 “(a) DEFINITIONS.—In this section:

3 “(1) VULNERABILITY DISCLOSURE REPORT.—

4 The term ‘vulnerability disclosure report’ means a  
5 disclosure of a security vulnerability (as that term is  
6 defined in section 1501(17) of title 6, United States  
7 Code) made to an agency by a reporter.

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

12 “(b) RESPONSIBILITIES OF OMB.—

13 “(1) LIMITATION ON LEGAL ACTION.—The Di-  
14 rector of the Office of Management and Budget, in  
15 consultation with the Attorney General, shall issue  
16 guidance to agencies to not recommend or pursue  
17 legal action against a reporter or an individual  
18 that—

19 “(A) conducts a security research activity  
20 that the head of the agency determines rep-  
21 resents a good faith effort to identify and re-  
22 port security vulnerabilities in Federal informa-  
23 tion systems; or

24 “(B) is otherwise authorized under the vul-  
25 nerability disclosure policy of the agency devel-  
26 oped under subsection (d)(2).

1           “(2) SHARING INFORMATION WITH CISA.—The  
2           Director of the Office of Management and Budget,  
3           in coordination with the Director of the Cybersecu-  
4           rity and Infrastructure Security Agency and in con-  
5           sultation with the National Cyber Director, shall  
6           issue guidance to agencies on sharing relevant infor-  
7           mation in a consistent, automated, and machine  
8           readable manner with the Director of the Cybersecu-  
9           rity and Infrastructure Security Agency, including—

10                   “(A) any valid or credible vulnerability dis-  
11                   closure reports of newly discovered or not pub-  
12                   licly known vulnerabilities (including  
13                   misconfigurations) on commercial software or  
14                   services used by Federal information systems;

15                   “(B) information relating to vulnerability  
16                   disclosure, coordination, or remediation activi-  
17                   ties of an agency, particularly as those activities  
18                   relate to outside organizations—

19                           “(i) with which the head of the agency  
20                           believes the Director of the Cybersecurity  
21                           and Infrastructure Security Agency can as-  
22                           sist; or

23                           “(ii) about which the head of the  
24                           agency believes the Director of the Cyber-

1 security and Infrastructure Security Agen-  
2 cy should know; and

3 “(C) any other information with respect to  
4 which the head of the agency determines helpful  
5 or necessary to involve the Director of the Cy-  
6 bersecurity and Infrastructure Security Agency.

7 “(3) AGENCY VULNERABILITY DISCLOSURE  
8 POLICIES.—The Director shall issue guidance to  
9 agencies on the required minimum scope of agency  
10 systems covered by the vulnerability disclosure policy  
11 of an agency required under subsection (d)(2).

12 “(c) RESPONSIBILITIES OF CISA.—The Director of  
13 the Cybersecurity and Infrastructure Security Agency  
14 shall—

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

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

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

1           “(4) as appropriate, implement the require-  
2           ments of this section, in accordance with authorities  
3           set out in section 3553(b)(8), as a shared service  
4           available to agencies.

5           “(d) RESPONSIBILITIES OF AGENCIES.—

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

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;

22                           “(ii) the type of information system  
23                           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; and

4 “(iv) the disclosure policy of the agen-  
5 cy for sensitive information;

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

8 “(i) how the reporter should submit  
9 the vulnerability disclosure report; and

10 “(ii) if the vulnerability disclosure re-  
11 port is not anonymous, when the reporter  
12 should anticipate an acknowledgment of re-  
13 ceipt of the vulnerability disclosure report  
14 by the agency;

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

17 “(D) be mature in scope, covering all inter-  
18 net accessible Federal information systems used  
19 or operated by that agency or on behalf of that  
20 agency.

21 “(3) IDENTIFIED VULNERABILITIES.—The head  
22 of each agency shall consider vulnerabilities reported  
23 under paragraph (2) and, commensurate with the  
24 risk posed by the vulnerability, address such vulner-  
25 ability using the vulnerability management process

1 of the agency in order to track and remediate the  
2 vulnerability.

3 “(e) CONGRESSIONAL REPORTING.—Not later than  
4 90 days after the date of the enactment of the Federal  
5 Information Security Modernization Act of 2022, and an-  
6 nually thereafter for a 3-year period, the Director of the  
7 Cybersecurity and Infrastructure Security Agency, in con-  
8 sultation with the Director and impacted agencies, shall  
9 provide to the Committee on Homeland Security and Gov-  
10 ernmental Affairs of the Senate and the Committee on  
11 Oversight and Reform of the House of Representatives a  
12 briefing on the status of the use of vulnerability disclosure  
13 policies under this section at agencies, including, with re-  
14 spect to the guidance issued under subsection (b)(3), an  
15 identification of the agencies that are compliant and not  
16 compliant.

17 “(f) EXEMPTIONS.—The authorities and functions of  
18 the Director and Director of the Cybersecurity and Infra-  
19 structure Security Agency under this section shall not  
20 apply to national security systems.

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

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

3           “(2) to the Director of National Intelligence in  
4           the case of systems described in section  
5           3553(e)(3).”.

6           (b) SUNSET.—This section shall sunset and any  
7           amendments made by this section shall be repealed on the  
8           date that is 10 years after the date of the enactment of  
9           this Act.

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

          “3559B. Federal vulnerability disclosure programs.”.

14          **SEC. 206. IMPLEMENTING ZERO TRUST ARCHITECTURE.**

15          (a) GUIDANCE.—The Director shall maintain guid-  
16          ance on the adoption of zero trust architecture and not  
17          later than 2 years after the date of the enactment of this  
18          Act, provide an update to the appropriate congressional  
19          committees on progress in increasing the internal defenses  
20          of agency systems through such adoption across the gov-  
21          ernment, including—

22                 (1) shifting away from “trusted networks” to  
23                 implement security controls based on a presumption  
24                 of compromise;



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

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

6           (4) identifying incidents quickly;

7           (5) isolating and removing unauthorized entities  
8           from agency systems as quickly as practicable, ac-  
9           counting for intelligence or law enforcement pur-  
10          poses;

11          (6) otherwise increasing the resource costs for  
12          entities that cause incidents to be successful; and

13          (7) a summary of the agency progress reports  
14          required under subsection (b).

15          (b) AGENCY PROGRESS REPORTS.—Not later than  
16          270 days after the date of the enactment of this Act, the  
17          head of each agency shall submit to the Director a  
18          progress report on implementing an information security  
19          program based on a zero trust architecture, which shall  
20          include—

21                (1) a description of any steps the agency has  
22                completed, including progress toward achieving any  
23                requirements issued by the Director, including the  
24                adoption of any models or reference architecture;

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

4           (3) a schedule to implement any planned activi-  
5           ties.

6   **SEC. 207. GAO AUTOMATION REPORT.**

7           Not later than 2 years after the date of the enact-  
8           ment of this Act, the Comptroller General of the United  
9           States shall perform a study and submit to the Commit-  
10          tees on Oversight and Reform, Homeland Security, and  
11          Science, Space, and Technology of the House of Rep-  
12          resentatives and the Committees on Homeland Security  
13          and Governmental Affairs and Commerce, Science, and  
14          Transportation of the Senate a report on the use of auto-  
15          mation and machine-readable data across the Federal  
16          Government for cybersecurity purposes, including the  
17          automated updating of cybersecurity tools, sensors, or  
18          processes employed by agencies under paragraphs (1),  
19          (5)(C), and (8)(B) of section 3554(b) of title 44, United  
20          States Code, as amended by this Act.

21   **SEC. 208. EXTENSION OF FEDERAL ACQUISITION SECURITY**  
22                                   **COUNCIL.**

23          (a) **EXTENSION.**—Section 1328 of title 41, United  
24          States Code, is amended by striking “the date that” and  
25          all that follows and inserting “December 31, 2026.”.

1           (b) EXTENSION.—Section 4713(j) of title 41, United  
2 States Code, is amended by striking “the date that” and  
3 all that follows and inserting “December 31, 2026.”.

4           (c) DESIGNATION.—Section 1322(c)(1) of title 41,  
5 United States Code, is amended by striking “Not later  
6 than” and all that follows through the end of the para-  
7 graph and inserting the following: “The Director of OMB  
8 shall designate the Federal Chief Information Security Of-  
9 ficer appointed by the President under section 3607 of  
10 title 44, or an equivalent senior-level official from the Of-  
11 fice of Management and Budget if the position is vacant,  
12 to serve as the Chairperson of the Council.”.

13           (d) REQUIREMENT.—Subsection 1326(b) of title 41,  
14 United States Code, is amended—

15                 (1) in paragraph (5), by striking “; and” and  
16 inserting a semicolon;

17                 (2) by redesignating paragraph (6) as para-  
18 graph (7); and

19                 (3) by inserting after paragraph (5) the fol-  
20 lowing new paragraph:

21                         “(6) maintaining an up-to-date and accurate in-  
22 ventory of software in use by the agency and, when  
23 available, the components of such software, including  
24 any available Software Bills of Materials, as applica-  
25 ble, that can be communicated when requested to

1 the Federal Acquisition Security Council, the Na-  
2 tional Cybersecurity Director, or the Secretary of  
3 Homeland Security acting through the Director of  
4 Cybersecurity and Infrastructure Security Agency;  
5 and”.

6 **SEC. 209. RENAMING OF OFFICE OF THE FEDERAL CHIEF**  
7 **INFORMATION OFFICER.**

8 (a) DEFINITIONS.—Section 3601 of title 44, United  
9 States Code, is amended—

10 (1) by striking paragraph (1); and

11 (2) by redesignating paragraphs (2) through  
12 (8) as paragraphs (1) through (7), respectively.

13 (b) OFFICE OF ELECTRONIC GOVERNMENT.—Section  
14 3602 of title 44, United States Code, is amended—

15 (1) in the heading, by striking “**Office of**  
16 **Electronic Government**” and inserting “**Of-**  
17 **ice of the Federal Chief Information Offi-**  
18 **cer**”;

19 (2) in subsection (a), by striking “Office of  
20 Electronic Government” and inserting “Office of the  
21 Federal Chief Information Officer”;

22 (3) in subsection (b), by striking “an Adminis-  
23 trator” and inserting “a Federal Chief Information  
24 Officer”;

1 (4) in subsection (c), by striking “The Adminis-  
2 trator” and inserting “The Federal Chief Informa-  
3 tion Officer”;

4 (5) in subsection (d), by striking “The Adminis-  
5 trator” and inserting “The Federal Chief Informa-  
6 tion Officer”;

7 (6) in subsection (e), by striking “The Adminis-  
8 trator” and inserting “The Federal Chief Informa-  
9 tion Officer”;

10 (7) in subsection (f)—

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

14 (B) in paragraph (16), by striking “the  
15 Office of Electronic Government” and inserting  
16 “the Office of the Federal Chief Information  
17 Officer”; and

18 (C) by adding at the end the following new  
19 paragraph:

20 “(18) Oversee the Federal Chief Information  
21 Security Officer.”; and

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

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

3 (1) in subsection (b)(2), by striking “The Ad-  
4 ministrator of the Office of Electronic Government”  
5 and inserting “The Federal Chief Information Offi-  
6 cer”;

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

11 (3) in subsection (f)—

12 (A) in paragraph (3), by striking “the Ad-  
13 ministrator” and inserting “the Federal Chief  
14 Information Officer”; and

15 (B) in paragraph (5), by striking “the Ad-  
16 ministrator” and inserting “the Federal Chief  
17 Information Officer”.

18 (d) E-GOVERNMENT FUND.—Section 3604 of title  
19 44, United States Code, is amended—

20 (1) in paragraph (2) of subsection (a), by strik-  
21 ing “the Administrator of the Office of Electronic  
22 Government” and inserting “the Federal Chief In-  
23 formation Officer”;

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

4           (3) in subsection (c), by striking “the Adminis-  
5           trator” and inserting “the Federal Chief Informa-  
6           tion Officer”.

7           (e) PROGRAM TO ENCOURAGE INNOVATIVE SOLU-  
8           TIONS TO ENHANCE ELECTRONIC GOVERNMENT SERV-  
9           ICES AND PROCESSES.—Section 3605 of title 44, United  
10          States Code, is amended—

11           (1) in subsection (a), by striking “The Adminis-  
12           trator” and inserting “The Federal Chief Informa-  
13           tion Officer”;

14           (2) in subsection (b), by striking “, the Admin-  
15           istrator,” and inserting “, the Federal Chief Infor-  
16           mation Officer,”; and

17           (3) in subsection (c)—

18           (A) in paragraph (1)—

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

22           (ii) by striking “proposals submitted  
23           to the Administrator” and inserting “pro-  
24           posals submitted to the Federal Chief In-  
25           formation Officer”;

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

4 (C) in paragraph (4), by striking “the Ad-  
5 ministrator” and inserting “the Federal Chief  
6 Information Officer”; and

7 (f) E-GOVERNMENT REPORT.—Section 3606 of title  
8 44, United States Code, is amended—

9 (1) in the heading, by striking “**E-Govern-**  
10 **ment**” and inserting “**Annual**”; and

11 (2) in subsection (a), by striking “an E-Gov-  
12 ernment status report to the Committee on Govern-  
13 mental Affairs of the Senate and the Committee on  
14 Government Reform of the House of Representa-  
15 tives” and inserting “a report to the Committee on  
16 Homeland Security and Governmental Affairs of the  
17 Senate and the Committee on Oversight and Govern-  
18 ment Reform of the House of Representatives”.

19 (g) TREATMENT OF INCUMBENT.—The individual  
20 serving as the Administrator of the Office of Electronic  
21 Government under section 3602 of title 44, United States  
22 Code, as of the date of the enactment of this Act, may  
23 continue to serve as the Federal Chief Information Officer  
24 commencing as of that date, without further appointment  
25 under such section.



1 (h) REFERENCES.—Any reference to the Adminis-  
2 trator of the Office of Electronic Government in any law,  
3 regulation, document, record, or other paper of the United  
4 States shall be deemed to be a reference to the Federal  
5 Chief Information Officer.

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

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

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

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

13 **SEC. 210. FEDERAL CHIEF INFORMATION SECURITY OFFI-**  
14 **CER.**

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

18 **“§ 3607. Federal chief information security officer**

19 “(a) ESTABLISHMENT.—There is established in the  
20 Office of the Federal Chief Information Officer of the Of-  
21 fice of Management and Budget a Federal Chief Informa-  
22 tion Security Officer, who shall be appointed by the Presi-  
23 dent.

24 “(b) DUTIES.—The Federal Chief Information Secu-  
25 rity Officer shall report to the Federal Chief Information

1 Officer, and assist the Chief Information Officer in car-  
2 rying out—

3 “(1) all functions under this chapter;

4 “(2) all functions assigned to the Director  
5 under title II of the E–Government Act of 2002;

6 “(3) other electronic government initiatives,  
7 consistent with other statutes; and

8 “(4) other initiatives determined by the Chief  
9 Information Officer.

10 “(c) ADDITIONAL DUTIES.—The Federal Chief Infor-  
11 mation Security Officer shall work with the Chief Informa-  
12 tion Officer to oversee implementation of electronic Gov-  
13 ernment under the E–Government Act of 2002, and other  
14 relevant statutes, in a manner consistent with law, relating  
15 to—

16 “(1) cybersecurity strategy, policy, and oper-  
17 ations, including the performance of the duties of  
18 the Director under subchapter II of chapter 35;

19 “(2) the development of enterprise architec-  
20 tures;

21 “(3) information security;

22 “(4) privacy;

23 “(5) access to, dissemination of, and preserva-  
24 tion of Government information; and

1           “(6) other areas of electronic Government as  
2           determined by the Federal Chief Information Offi-  
3           cer.

4           “(d) ASSISTANCE.—The Federal Chief Information  
5           Security Officer shall assist the Federal Chief Information  
6           Officer in the performance of electronic Government func-  
7           tions as described in section 3602(f).”.

8           (b) DEPUTY NATIONAL CYBER DIRECTOR.—Section  
9           1752 of the William M. (Mac) Thornberry National De-  
10          fense Authorization Act for Fiscal Year 2021 (6 U.S.C.  
11          1500; 134 Stat. 4144) is amended by adding at the end  
12          the following new subsection:

13          “(h) DEPUTY DIRECTOR.—There shall be a Deputy  
14          National Cyber Director for Agency Strategy, Capabilities,  
15          and Budget, who shall be the Federal Chief Information  
16          Security Officer appointed by the President under section  
17          3607 of title 44, United States Code, and shall report to  
18          the Director and assist the office in carrying out the fol-  
19          lowing duties as it applies to the protection of Federal in-  
20          formation systems by the agencies—

21                  “(1) the preparation and oversight over the im-  
22                  plementation of national cyber policy and strategy  
23                  under subsection (c)(1)(C)(i);

1           “(2) the formation and issuance of rec-  
2           ommendations to agencies on resource allocations  
3           and policies under subsection (c)(1)(C)(ii);

4           “(3) reviewing annual budget proposals and  
5           making related recommendations under subsection  
6           (c)(1)(C)(iii);

7           “(4) the functions, as determined necessary, of  
8           the National Cyber Director under subchapter II of  
9           chapter 35 of title 44, United States Code; and

10          “(5) other initiatives determined by the Direc-  
11          tor, or to be necessary to coordinate with the Office  
12          by the Federal Chief Information Officer.”.

13          (c) CLERICAL AMENDMENT.—The table of sections  
14          for chapter 36 of title 44, United States Code, is amended  
15          by adding after the item relating to section 3606 the fol-  
16          lowing:

          “3607. Federal chief information security officer.”.

17          **SEC. 211. EXTENSION OF CHIEF DATA OFFICER COUNCIL.**

18          Section 3520A(e)(2) of title 44, United States Code,  
19          is amended by striking “upon the expiration of the 2-year  
20          period that begins on the date the Comptroller General  
21          submits the report under paragraph (1) to Congress” and  
22          inserting “January 31, 2030”.

1 **SEC. 212. COUNCIL OF THE INSPECTORS GENERAL ON IN-**  
2 **TEGRITY AND EFFICIENCY DASHBOARD.**

3 Section 11(e)(2) of the Inspector General Act of 1978  
4 (5 U.S.C. App.) is amended—

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

7 (2) by redesignating subparagraph (B) as sub-  
8 paragraph (C); and

9 (3) by inserting after subparagraph (A) the fol-  
10 lowing:

11 “(B) that shall include a dashboard of  
12 open information security recommendations  
13 identified in the independent evaluations re-  
14 quired by section 3555(a) of title 44, United  
15 States Code; and”.

16 **SEC. 213. QUANTITATIVE CYBERSECURITY METRICS.**

17 (a) **DEFINITION OF COVERED METRICS.**—In this sec-  
18 tion, the term “covered metrics” means the metrics estab-  
19 lished, reviewed, and updated under section 224(c) of the  
20 Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

21 (b) **UPDATING AND ESTABLISHING METRICS.**—Not  
22 later than 1 year after the date of the enactment of this  
23 Act, the Director of the Cybersecurity and Infrastructure  
24 Security Agency, in coordination with the Director and the  
25 National Cyber Director and consulting with the Director

1 of the National Institute of Standards and Technology,  
2 shall—

3 (1) evaluate any covered metrics established as  
4 of the date of the enactment of this Act; and

5 (2) as appropriate and pursuant to section  
6 224(c) of the Cybersecurity Act of 2015 (6 U.S.C.  
7 1522(c))—

8 (A) update the covered metrics; and

9 (B) establish new covered metrics.

10 (c) IMPLEMENTATION.—

11 (1) IN GENERAL.—Not later than 540 days  
12 after the date of the enactment of this Act, the Di-  
13 rector, in coordination with the Director of the Cy-  
14 bersecurity and Infrastructure Security Agency,  
15 shall promulgate guidance that requires each agency  
16 to use covered metrics to track trends in the cyber-  
17 security and incident response capabilities of the  
18 agency.

19 (2) PERFORMANCE DEMONSTRATION.—The  
20 guidance issued under paragraph (1) and any subse-  
21 quent guidance shall require agencies to share with  
22 the Director of the Cybersecurity and Infrastructure  
23 Security Agency data demonstrating the perform-  
24 ance of the agency using the covered metrics in-  
25 cluded in the guidance.

1           (3) PENETRATION TESTS.—On not less than 2  
2           occasions during the 2-year period following the date  
3           on which guidance is promulgated under paragraph  
4           (1), the Director shall ensure that not less than 3  
5           agencies are subjected to substantially similar pene-  
6           tration tests, as determined by the Director, in co-  
7           ordination with the Director of the Cybersecurity  
8           and Infrastructure Security Agency, in order to vali-  
9           date the utility of the covered metrics.

10           (4) ANALYSIS CAPACITY.—The Director of the  
11           Cybersecurity and Infrastructure Security Agency  
12           shall develop a capability that allows for the analysis  
13           of the covered metrics, including cross-agency per-  
14           formance of agency cybersecurity and incident re-  
15           sponse capability trends.

16           (d) CONGRESSIONAL REPORT.—Not later than 1 year  
17           after the date of the enactment of this Act, the Director  
18           of the Cybersecurity and Infrastructure Security Agency,  
19           in coordination with the Director, shall submit to the ap-  
20           propriate congressional committees a report on the utility  
21           of the covered metrics.

22           (e) FEDERAL CYBERSECURITY ENHANCEMENT ACT  
23           OF 2015 UPDATES.—The Federal Cybersecurity Enhance-  
24           ment Act of 2015 (6 U.S.C. 1521 et seq) is amended—

1 (1) in section 222(3)(B), by inserting “and the  
2 Committee on Oversight and Reform” before “of the  
3 House of Representatives”; and

4 (2) in section 224—

5 (A) by amending subsection (c) to read as  
6 follows:

7 “(c) IMPROVED METRICS.—The Director of the Cy-  
8 bersecurity and Infrastructure Security Agency, in coordi-  
9 nation with the Director, shall establish, review, and up-  
10 date metrics to measure the cybersecurity and incident re-  
11 sponse capabilities of agencies in accordance with the re-  
12 sponsibilities of agencies under section 3554 of title 44,  
13 United States Code.”;

14 (B) by striking subsection (e); and

15 (C) by redesignating subsection (f) as sub-  
16 section (e).

17 **TITLE III—PILOT PROGRAMS TO**  
18 **ENHANCE FEDERAL CYBER-**  
19 **SECURITY**

20 **SEC. 301. RISK-BASED BUDGET PILOT.**

21 (a) DEFINITIONS.—In this section:

22 (1) APPROPRIATE CONGRESSIONAL COMMIT-  
23 TEES.—The term “appropriate congressional com-  
24 mittees” means—



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

4 (B) the Committee on Homeland Security,  
5 the Committee on Oversight and Reform, and  
6 the Committee on Appropriations of the House  
7 of Representatives.

8 (2) INFORMATION TECHNOLOGY.—The term  
9 “information technology”—

10 (A) has the meaning given the term in sec-  
11 tion 11101 of title 40, United States Code; and

12 (B) includes the hardware and software  
13 systems of an agency that monitor and control  
14 physical equipment and processes of the agency.

15 (3) RISK-BASED BUDGET.—The term “risk-  
16 based budget” means a budget—

17 (A) developed by identifying and  
18 prioritizing cybersecurity risks and  
19 vulnerabilities, including impact on agency oper-  
20 ations in the case of a cyber attack, through  
21 analysis of cyber threat intelligence, incident  
22 data, and tactics, techniques, procedures, and  
23 capabilities of cyber threats; and

1 (B) that allocates resources based on the  
2 risks identified and prioritized under subpara-  
3 graph (A).

4 (b) ESTABLISHMENT OF RISK-BASED BUDGET  
5 PILOT.—

6 (1) IN GENERAL.—

7 (A) MODEL.—Not later than 1 year after  
8 the first publication of the budget submitted by  
9 the President under section 1105 of title 31,  
10 United States Code, following the date of the  
11 enactment of this Act, the Director, in consulta-  
12 tion with the Director of the Cybersecurity and  
13 Infrastructure Security Agency and the Na-  
14 tional Cyber Director and in coordination with  
15 the Director of the National Institute of Stand-  
16 ards and Technology, shall conduct a pilot for  
17 creating a risk-based budget for cybersecurity  
18 spending.

19 (B) CONTENTS OF PILOT.—The pilot re-  
20 quired to be developed under this paragraph  
21 shall—

22 (i) consider Federal and non-Federal  
23 cyber threat intelligence products, where  
24 available, to identify threats,  
25 vulnerabilities, and risks;

1 (ii) consider the impact on agency op-  
2 erations of incidents, including the  
3 interconnectivity to other agency systems  
4 and the operations of other agencies;

5 (iii) indicate where resources should  
6 be allocated to have the greatest impact on  
7 mitigating current and future threats and  
8 current and future cybersecurity capabili-  
9 ties;

10 (iv) be used to inform acquisition and  
11 sustainment of—

12 (I) information technology and  
13 cybersecurity tools;

14 (II) information technology and  
15 cybersecurity architectures;

16 (III) information technology and  
17 cybersecurity personnel; and

18 (IV) cybersecurity and informa-  
19 tion technology concepts of operations;  
20 and

21 (v) be used to evaluate and inform  
22 government-wide cybersecurity programs of  
23 the Department of Homeland Security.

24 (2) REPORTS.—Not later than 3 years after the  
25 first publication of the budget submitted by the

1 President under section 1105 of title 31, United  
2 States Code, following the date of the enactment of  
3 this Act, the Director shall submit a report to Con-  
4 gress on the implementation of the pilot for risk-  
5 based budgeting for cybersecurity spending, an as-  
6 sessment of agency implementation, and an evalua-  
7 tion of whether the risk-based budget helps to miti-  
8 gate cybersecurity vulnerabilities.

9 (3) GAO REPORT.—Not later than 4 years  
10 after the first publication of the budget submitted by  
11 the President under section 1105 of title 31, United  
12 States Code, following the date of the enactment of  
13 this Act, the Comptroller General of the United  
14 States shall submit to the appropriate congressional  
15 committees a report that includes—

16 (A) an evaluation of the success of pilot  
17 agencies in implementing risk-based budgets;

18 (B) an evaluation of whether the risk-  
19 based budgets developed by pilot agencies are  
20 effective at informing Federal Government-wide  
21 cybersecurity programs; and

22 (C) any other information relating to risk-  
23 based budgets the Comptroller General deter-  
24 mines appropriate.

1 **SEC. 302. ACTIVE CYBER DEFENSIVE STUDY.**

2 (a) DEFINITION.—In this section, the term “active  
3 defense technique” has the meaning given in guidance  
4 issued by the Director, in coordination with the Attorney  
5 General.

6 (b) STUDY.—Not later than 180 days after the date  
7 of the enactment of this Act, the Director of the Cyberse-  
8 curity and Infrastructure Security Agency, in coordination  
9 with the Director and the National Cyber Director, shall  
10 perform a study and submit to the Committees on Over-  
11 sight and Reform and Homeland Security of the House  
12 of Representatives and the Committee on Homeland Secu-  
13 rity and Governmental Affairs of the Senate a report on  
14 the use of active defense techniques to enhance the secu-  
15 rity of agencies, which shall include—

16 (1) a review of legal restrictions on the use of  
17 different active cyber defense techniques in Federal  
18 environments, in consultation with the Attorney  
19 General;

20 (2) an evaluation of—

21 (A) the efficacy of a selection of active de-  
22 fense techniques determined by the Director of  
23 the Cybersecurity and Infrastructure Security  
24 Agency; and

1 (B) factors that impact the efficacy of the  
2 active defense techniques evaluated under sub-  
3 paragraph (A);

4 (3) recommendations on safeguards and proce-  
5 dures that shall be established to require that active  
6 defense techniques are adequately coordinated to en-  
7 sure that active defense techniques do not impede  
8 agency operations and mission delivery, threat re-  
9 sponse efforts, criminal investigations, and national  
10 security activities, including intelligence collection;  
11 and

12 (4) the development of a framework for the use  
13 of different active defense techniques by agencies.

14 **SEC. 303. SECURITY OPERATIONS CENTER AS A SERVICE**  
15 **PILOT.**

16 (a) PLAN.—Not later than 1 year after the date of  
17 the enactment of this Act, the Director of the Cybersecu-  
18 rity and Infrastructure Security Agency shall develop a  
19 plan to establish a centralized Federal security operations  
20 center shared service offering within the Cybersecurity  
21 and Infrastructure Security Agency.

22 (b) CONTENTS.—The plan required under subsection  
23 (a) shall include considerations for—

24 (1) collecting, organizing, and analyzing agency  
25 information system data in real time;

1           (2) staffing and resources; and

2           (3) appropriate interagency agreements, con-  
3           cepts of operations, and governance plans, including  
4           alignment with existing shared services operations  
5           and policy.

6           (c) PILOT PROGRAM.—

7           (1) IN GENERAL.—Not later than 180 days  
8           after the date on which the plan required under sub-  
9           section (a) is developed, the Director of the Cyberse-  
10          curity and Infrastructure Security Agency, in con-  
11          sultation with the Director of the Office of Manage-  
12          ment and Budget, shall enter into a 1-year agree-  
13          ment with not less than 2 agencies to offer a secu-  
14          rity operations center as a shared service.

15          (2) ADDITIONAL AGREEMENTS.—After the date  
16          on which the briefing required under subsection  
17          (d)(1) is provided, the Director of the Cybersecurity  
18          and Infrastructure Security Agency, in consultation  
19          with the Director of the Office of Management and  
20          Budget, may enter into additional 1-year agreements  
21          described in paragraph (1) with agencies.

22          (d) BRIEFING AND REPORT.—

23          (1) BRIEFING.—Not later than 270 days after  
24          the date of the enactment of this Act, the Director  
25          of the Cybersecurity and Infrastructure Security

1 Agency shall provide to appropriate congressional  
2 committees a briefing on the parameters of any 1-  
3 year agreements entered into under subsection  
4 (c)(1).

5 (2) REPORT.—Not later than 90 days after the  
6 date on which the first 1-year agreement entered  
7 into under subsection (c) expires, the Director of the  
8 Cybersecurity and Infrastructure Security Agency  
9 shall submit to appropriate congressional committees  
10 a report on—

11 (A) the agreement; and

12 (B) any additional agreements entered into  
13 with agencies under subsection (c).

14 **SEC. 304. DETECTION AND RESPONSE AS A SERVICE PILOT.**

15 (a) PURPOSE.—The Cybersecurity and Infrastruc-  
16 ture Security Agency is directed to establish and conduct  
17 a pilot to determine the feasibility, value, and efficacy of  
18 providing detection and response capabilities as a shared  
19 service to agencies to reduce costs, enhance interoper-  
20 ability, and continuously detect and mitigate threat activ-  
21 ity on Federal networks.

22 (b) PLAN.—Not later than 90 days after the date of  
23 the enactment of this Act, the Director of the Cybersecu-  
24 rity and Infrastructure Security Agency shall develop a  
25 plan to establish a centralized detection and response



1 shared service offering within the Cybersecurity and Infra-  
2 structure Security Agency.

3 (c) CONTENTS.—The plan required under subsection  
4 (b) shall include considerations for—

5 (1) understanding and assessing the full extent  
6 of endpoints across the Federal civilian environment;

7 (2) maximizing the value of existing agency in-  
8 vestments in endpoint detection and response tools  
9 and services;

10 (3) aggregating the available contract vehicles  
11 and options that provide agencies with appropriate  
12 capability for their environment and architecture;

13 (4) equipping all endpoints and services of pilot  
14 agencies with endpoint detection and response pro-  
15 grams;

16 (5) where appropriate, aggregating network,  
17 cloud, and endpoint data from both within the agen-  
18 cy and across agencies to provide enterprise-wide  
19 monitoring of the network to detect abnormal net-  
20 work behavior and automate defensive capabilities;  
21 and

22 (6) appropriate interagency agreements, con-  
23 cepts of operations, and governance plans, including  
24 alignment with existing shared services operations  
25 and policy.

1 (d) PILOT PROGRAM.—

2 (1) IN GENERAL.—Not later than 180 days  
3 after the date on which the plan required under sub-  
4 section (b) is developed, the Director of the Cyberse-  
5 curity and Infrastructure Security Agency, in con-  
6 sultation with the Director, shall enter into a 1-year  
7 agreement with not less than 2 agencies to offer de-  
8 tection and response as a shared service.

9 (2) ADDITIONAL AGREEMENTS.—After the date  
10 on which the briefing required under subsection  
11 (e)(1) is provided, the Director of the Cybersecurity  
12 and Infrastructure Security Agency, in consultation  
13 with the Director, may enter into additional 1-year  
14 agreements described in paragraph (1) with agen-  
15 cies.

16 (e) BRIEFING AND REPORT.—

17 (1) BRIEFING.—Not later than 270 days after  
18 the date of the enactment of this Act, the Director  
19 of the Cybersecurity and Infrastructure Security  
20 Agency shall provide to the Committee on Homeland  
21 Security and Governmental Affairs of the Senate  
22 and the Committee on Homeland Security and the  
23 Committee on Oversight and Reform of the House  
24 of Representatives a briefing on the parameters of

1 any 1-year agreements entered into under subsection  
2 (d)(1).

3 (2) REPORT.—Not later than 90 days after the  
4 date on which the first 1-year agreement entered  
5 into under subsection (d) expires, the Director of the  
6 Cybersecurity and Infrastructure Security Agency  
7 shall submit to the Committee on Homeland Secu-  
8 rity and Governmental Affairs of the Senate and the  
9 Committee on Homeland Security and the Com-  
10 mittee on Oversight and Reform of the House of  
11 Representatives a report on—

12 (A) the agreement; and

13 (B) any additional agreements entered into  
14 with agencies under subsection (d).

