

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: To modernize Federal information security management, to amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and to make technical corrections to the Homeland Security Act of 2002.

**IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.**

**H. R. 4350**

To authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT intended to be proposed by Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, Mr. RUBIO, and Ms. COLLINS) to the amendment (No. 3867) proposed by Mr. REED

Viz:

1 At the end, add the following:

1 **DIVISION E—FEDERAL INFOR-**  
2 **MATION SECURITY MOD-**  
3 **ERNIZATION ACT OF 2021**

4 **SEC. 5101. SHORT TITLE.**

5 This division may be cited as the “Federal Informa-  
6 tion Security Modernization Act of 2021”.

7 **SEC. 5102. DEFINITIONS.**

8 In this division, unless otherwise specified:

9 (1) **ADDITIONAL CYBERSECURITY PROCE-**  
10 **DURE.**—The term “additional cybersecurity proce-  
11 dure” has the meaning given the term in section  
12 3552(b) of title 44, United States Code, as amended  
13 by this division.

14 (2) **AGENCY.**—The term “agency” has the  
15 meaning given the term in section 3502 of title 44,  
16 United States Code.

17 (3) **APPROPRIATE CONGRESSIONAL COMMIT-**  
18 **TEES.**—The term “appropriate congressional com-  
19 mittees” means—

20 (A) the Committee on Homeland Security  
21 and Governmental Affairs of the Senate;

22 (B) the Committee on Oversight and Re-  
23 form of the House of Representatives; and

24 (C) the Committee on Homeland Security  
25 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 division.

15          (8) THREAT HUNTING.—The term “threat  
16          hunting” means proactively and iteratively searching  
17          for threats to systems that evade detection by auto-  
18          mated threat detection systems.

## 19          **TITLE LI—UPDATES TO FISMA**

### 20          **SEC. 5121. TITLE 44 AMENDMENTS.**

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

23                  (1) in section 3504—

24                          (A) in subsection (a)(1)(B)—

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

3 “(v) confidentiality, disclosure, and sharing  
4 of information;”;

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

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

9 “(vi) in consultation with the National  
10 Cyber Director and the Director of the Cyberse-  
11 curity and Infrastructure Security Agency, se-  
12 curity of information; and”;

13 (B) in subsection (g), by striking para-  
14 graph (1) and inserting the following:

15 “(1) with respect to information collected or  
16 maintained by or for agencies—

17 “(A) develop and oversee the implementa-  
18 tion of policies, principles, standards, and  
19 guidelines on privacy, confidentiality, disclosure,  
20 and sharing of the information; and

21 “(B) in consultation with the National  
22 Cyber Director and the Director of the Cyberse-  
23 curity and Infrastructure Security Agency, de-  
24 velop and oversee policies, principles, standards,

1 and guidelines on security of the information;  
2 and”; and

3 (C) in subsection (h)(1)—

4 (i) in the matter preceding subpara-  
5 graph (A)—

6 (I) by inserting “the Director of  
7 the Cybersecurity and Infrastructure  
8 Security Agency and the National  
9 Cyber Director,” before “the Direc-  
10 tor”; and

11 (II) by inserting a comma before  
12 “and the Administrator”; and

13 (ii) in subparagraph (A), by inserting  
14 “security and” after “information tech-  
15 nology”;

16 (2) in section 3505—

17 (A) in paragraph (3) of the first subsection  
18 designated as subsection (c)—

19 (i) in subparagraph (B)—

20 (I) by inserting “the Director of  
21 the Cybersecurity and Infrastructure  
22 Security Agency, the National Cyber  
23 Director, and” before “the Comp-  
24 troller General”; and

25 (II) by striking “and” at the end;

1 (ii) in subparagraph (C)(v), by strik-  
2 ing the period at the end and inserting “;  
3 and”; and

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

6 “(D) maintained on a continual basis through  
7 the use of automation, machine-readable data, and  
8 scanning.”; and

9 (B) by striking the second subsection des-  
10 igned as subsection (c);

11 (3) in section 3506—

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

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

16 (4) in section 3513—

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

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

21 “(c) Each agency providing a written plan under sub-  
22 section (b) shall provide any portion of the written plan  
23 addressing information security or cybersecurity to the Di-  
24 rector of the Cybersecurity and Infrastructure Security  
25 Agency.”.

1 (b) SUBCHAPTER II DEFINITIONS.—

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

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

7 (B) by inserting before paragraph (2), as  
8 so redesignated, the following:

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

15 (C) by inserting after paragraph (6), as so  
16 redesignated, the following:

17 “(7) The term ‘high value asset’ means infor-  
18 mation or an information system that the head of an  
19 agency determines so critical to the agency that the  
20 loss or corruption of the information or the loss of  
21 access to the information system would have a seri-  
22 ous impact on the ability of the agency to perform  
23 the mission of the agency or conduct business.

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

4           (D) by inserting after paragraph (9), as so  
5           redesignated, the following:

6           “(10) The term ‘penetration test’ means a spe-  
7           cialized type of assessment that—

8           “(A) is conducted on an information sys-  
9           tem or a component of an information system;  
10          and

11          “(B) emulates an attack or other exploi-  
12          tation capability of a potential adversary, typi-  
13          cally under specific constraints, in order to  
14          identify any vulnerabilities of an information  
15          system or a component of an information sys-  
16          tem that could be exploited.”; and

17          (E) by inserting after paragraph (11), as  
18          so redesignated, the following:

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

23           (2) CONFORMING AMENDMENTS.—

24           (A) HOMELAND SECURITY ACT OF 2002.—

25           Section 1001(c)(1)(A) of the Homeland Secu-

1 rity Act of 2002 (6 U.S.C. 511(1)(A)) is  
2 amended by striking “section 3552(b)(5)” and  
3 inserting “section 3552(b)”.

4 (B) TITLE 10.—

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

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

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

18 (iv) SECTION 2339A.—Section  
19 2339a(e)(5) of title 10, United States  
20 Code, is amended by striking “section  
21 3552(b)(6)” and inserting “section  
22 3552(b)”.

23 (C) HIGH-PERFORMANCE COMPUTING ACT  
24 OF 1991.—Section 207(a) of the High-Perform-  
25 ance Computing Act of 1991 (15 U.S.C.

1 5527(a)) is amended by striking “section  
2 3552(b)(6)(A)(i)” and inserting “section  
3 3552(b)(9)(A)(i)”.

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

10 (E) NATIONAL DEFENSE AUTHORIZATION  
11 ACT FOR FISCAL YEAR 2013.—Section  
12 933(e)(1)(B) of the National Defense Author-  
13 ization Act for Fiscal Year 2013 (10 U.S.C.  
14 2224 note) is amended by striking “section  
15 3542(b)(2)” and inserting “section 3552(b)”.

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

21 (i) in section 806(e)(5) (10 U.S.C.  
22 2304 note), by striking “section 3542(b)”  
23 and inserting “section 3552(b)”;

24 (ii) in section 931(b)(3) (10 U.S.C.  
25 2223 note), by striking “section

1           3542(b)(2)” and inserting “section  
2           3552(b)”;

3                   (iii) in section 932(b)(2) (10 U.S.C.  
4           2224 note), by striking “section  
5           3542(b)(2)” and inserting “section  
6           3552(b)”.

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

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

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

19                   (ii) in subsection (f)—

20                           (I) in paragraph (3), by striking  
21                           “section 3532(1)” and inserting “sec-  
22                           tion 3552(b)”;

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

1 (c) SUBCHAPTER II AMENDMENTS.—Subchapter II  
2 of chapter 35 of title 44, United States Code, is amend-  
3 ed—

4 (1) in section 3551—

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

8 (B) by inserting after paragraph (2) the  
9 following:

10 “(3) recognize the role of the Cybersecurity and  
11 Infrastructure Security Agency as the lead entity for  
12 operational cybersecurity coordination across the  
13 Federal Government;”;

14 (C) in paragraph (5), as so redesignated,  
15 by striking “diagnose and improve” and insert-  
16 ing “integrate, deliver, diagnose, and improve”;

17 (D) in paragraph (6), as so redesignated,  
18 by striking “and” at the end;

19 (E) in paragraph (7), as so redesignated,  
20 by striking the period at the end and inserting  
21 a semi colon; and

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

23 “(8) recognize that each agency has specific  
24 mission requirements and, at times, unique cyberse-

1 security requirements to meet the mission of the agen-  
2 cy;

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

8 “(10) recognize that—

9 “(A) a holistic Federal cybersecurity model  
10 is necessary to account for differences between  
11 the missions and capabilities of agencies; and

12 “(B) in accounting for the differences de-  
13 scribed in subparagraph (A) and ensuring over-  
14 all Federal cybersecurity—

15 “(i) the Office of Management and  
16 Budget is the leader for policy development  
17 and oversight of Federal cybersecurity;

18 “(ii) the Cybersecurity and Infrastruc-  
19 ture Security Agency is the leader for im-  
20 plementing operations at agencies; and

21 “(iii) the National Cyber Director is  
22 responsible for developing the overall cy-  
23 bersecurity strategy of the United States  
24 and advising the President on matters re-  
25 lating to cybersecurity.”;

1 (2) in section 3553—

2 (A) by striking the section heading and in-  
3 sserting “**Authority and functions of the**  
4 **Director and the Director of the Cy-**  
5 **bersecurity and Infrastructure Secu-**  
6 **riety Agency**”.

7 (B) in subsection (a)—

8 (i) in paragraph (1), by inserting “in  
9 coordination with the Director of the Cy-  
10 bersecurity and Infrastructure Security  
11 Agency and the National Cyber Director,”  
12 before “developing and overseeing”;

13 (ii) in paragraph (5)—

14 (I) by inserting “, in consultation  
15 with the Director of the Cybersecurity  
16 and Infrastructure Security Agency  
17 and the National Cyber Director,” be-  
18 fore “agency compliance”; and

19 (II) by striking “and” at the end;

20 and

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

23 “(8) promoting, in consultation with the Direc-  
24 tor of the Cybersecurity and Infrastructure Security

1 Agency and the Director of the National Institute of  
2 Standards and Technology—

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 presumption of com-  
8 promise and least privilege principles to improve  
9 resiliency and timely response actions to inci-  
10 dents on Federal systems.”;

11 (C) in subsection (b)—

12 (i) by striking the subsection heading  
13 and inserting “CYBERSECURITY AND IN-  
14 FRASTRUCTURE SECURITY AGENCY”;

15 (ii) in the matter preceding paragraph  
16 (1), by striking “The Secretary, in con-  
17 sultation with the Director” and inserting  
18 “The Director of the Cybersecurity and In-  
19 frastructure Security Agency, in consulta-  
20 tion with the Director and the National  
21 Cyber Director”;

22 (iii) in paragraph (2)—

23 (I) in subparagraph (A), by in-  
24 serting “and reporting requirements

1 under subchapter IV of this title”  
2 after “section 3556”; and

3 (II) in subparagraph (D), by  
4 striking “the Director or Secretary”  
5 and inserting “the Director of the Cy-  
6 bersecurity and Infrastructure Secu-  
7 rity Agency”;

8 (iv) in paragraph (5), by striking “co-  
9 ordinating” and inserting “leading the co-  
10 ordination of”;

11 (v) in paragraph (8), by striking “the  
12 Secretary’s discretion” and inserting “the  
13 Director of the Cybersecurity and Infra-  
14 structure Security Agency’s discretion”;  
15 and

16 (vi) in paragraph (9), by striking “as  
17 the Director or the Secretary, in consulta-  
18 tion with the Director,” and inserting “as  
19 the Director of the Cybersecurity and In-  
20 frastructure Security Agency”;

21 (D) in subsection (c)—

22 (i) in the matter preceding paragraph  
23 (1), by striking “each year” and inserting  
24 “each year during which agencies are re-

1                   required to submit reports under section  
2                   3554(c)”;

3                   (ii) by striking paragraph (1);

4                   (iii) by redesignating paragraphs (2),  
5                   (3), and (4) as paragraphs (1), (2), and  
6                   (3), respectively;

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

9                   (v) by inserting after paragraph (3),  
10                  as so redesignated the following:

11                  “(4) a summary of each assessment of Federal  
12                  risk posture performed under subsection (i);” and

13                  (vi) in paragraph (5), by striking the  
14                  period at the end and inserting “; and”;

15                  (E) by redesignating subsections (i), (j),  
16                  (k), and (l) as subsections (j), (k), (l), and (m)  
17                  respectively;

18                  (F) by inserting after subsection (h) the  
19                  following:

20                  “(i) FEDERAL RISK ASSESSMENTS.—On an ongoing  
21                  and continuous basis, the Director of the Cybersecurity  
22                  and Infrastructure Security Agency shall perform assess-  
23                  ments of Federal risk posture using any available informa-  
24                  tion on the cybersecurity posture of agencies, and brief

1 the Director and National Cyber Director on the findings  
2 of those assessments including—

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

5 “(2) any vulnerability information relating to  
6 the systems of an agency that is known by the agen-  
7 cy;

8 “(3) analysis of incident information under sec-  
9 tion 3597;

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

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

14 “(6) evaluation of agency threat hunting re-  
15 sults;

16 “(7) evaluation of Federal and non-Federal  
17 threat intelligence;

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

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

22 “(10) any other information the Director of the  
23 Cybersecurity and Infrastructure Security Agency  
24 determines relevant.”; and

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

1 (i) by striking “regarding the spe-  
2 cific” and inserting “that includes a sum-  
3 mary of—

4 “(1) the specific”;

5 (ii) in paragraph (1), as so des-  
6 ignated, by striking the period at the end  
7 and inserting “; and” and

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

10 “(2) the trends identified in the Federal risk  
11 assessment performed under subsection (i).”; and

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

13 “(n) BINDING OPERATIONAL DIRECTIVES.—If the  
14 Director of the Cybersecurity and Infrastructure Security  
15 Agency issues a binding operational directive or an emer-  
16 gency directive under this section, not later than 2 days  
17 after the date on which the binding operational directive  
18 requires an agency to take an action, the Director of the  
19 Cybersecurity and Infrastructure Security Agency shall  
20 provide to the appropriate reporting entities the status of  
21 the implementation of the binding operational directive at  
22 the agency.”;

23 (3) in section 3554—

24 (A) in subsection (a)—

25 (i) in paragraph (1)—

1 (I) by redesignating subpara-  
2 graphs (A), (B), and (C) as subpara-  
3 graphs (B), (C), and (D), respectively;

4 (II) by inserting before subpara-  
5 graph (B), as so redesignated, the fol-  
6 lowing:

7 “(A) on an ongoing and continuous basis,  
8 performing agency system risk assessments  
9 that—

10 “(i) identify and document the high  
11 value assets of the agency using guidance  
12 from the Director;

13 “(ii) evaluate the data assets inven-  
14 toried under section 3511 for sensitivity to  
15 compromises in confidentiality, integrity,  
16 and availability;

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

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

## 21

1           “(v) evaluate the vulnerability of  
2 agency systems and data, including high  
3 value assets, including by analyzing—

4           “(I) the results of penetration  
5 testing performed by the Department  
6 of Homeland Security under section  
7 3553(b)(9);

8           “(II) the results of penetration  
9 testing performed under section  
10 3559A;

11           “(III) information provided to  
12 the agency through the vulnerability  
13 disclosure program of the agency  
14 under section 3559B;

15           “(IV) incidents; and

16           “(V) any other vulnerability in-  
17 formation relating to agency systems  
18 that is known to the agency;

19           “(vi) assess the impacts of potential  
20 agency incidents to agency systems, data,  
21 and operations based on the evaluations  
22 described in clauses (ii) and (iv) and the  
23 agency systems identified under clause  
24 (iii); and



1 (V) by adding at the end the fol-  
2 lowing:

3 “(E) providing an update on the ongoing  
4 and continuous assessment performed under  
5 subparagraph (A)—

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

9 “(ii) on a periodic basis, as deter-  
10 mined by guidance issued by the Director  
11 but not less frequently than annually, to—

12 “(I) the Director;

13 “(II) the Director of the Cyberse-  
14 curity and Infrastructure Security  
15 Agency; and

16 “(III) the National Cyber Direc-  
17 tor;

18 “(F) in consultation with the Director of  
19 the Cybersecurity and Infrastructure Security  
20 Agency and not less frequently than once every  
21 3 years, performing an evaluation of whether  
22 additional cybersecurity procedures are appro-  
23 priate for securing a system of, or under the  
24 supervision of, the agency, which shall—

1                   “(i) be completed considering the  
2                   agency system risk assessment performed  
3                   under subparagraph (A); and

4                   “(ii) include a specific evaluation for  
5                   high value assets;

6                   “(G) not later than 30 days after com-  
7                   pleting the evaluation performed under sub-  
8                   paragraph (F), providing the evaluation and an  
9                   implementation plan, if applicable, for using ad-  
10                  ditional cybersecurity procedures determined to  
11                  be appropriate to—

12                  “(i) the Director of the Cybersecurity  
13                  and Infrastructure Security Agency;

14                  “(ii) the Director; and

15                  “(iii) the National Cyber Director;

16                  and

17                  “(H) if the head of the agency determines  
18                  there is need for additional cybersecurity proce-  
19                  dures, ensuring that those additional cybersecu-  
20                  rity procedures are reflected in the budget re-  
21                  quest of the agency in accordance with the risk-  
22                  based cyber budget model developed pursuant  
23                  to section 3553(a)(7);”;

24                  (ii) in paragraph (2)—

1 (I) in subparagraph (A), by in-  
2 serting “in accordance with the agen-  
3 cy system risk assessment performed  
4 under paragraph (1)(A)” after “infor-  
5 mation systems”;

6 (II) in subparagraph (B)—

7 (aa) by striking “in accord-  
8 ance with standards” and insert-  
9 ing “in accordance with—

10 “(i) standards”; and

11 (bb) by adding at the end  
12 the following:

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

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

17 (III) in subparagraph (D), by in-  
18 serting “, through the use of penetra-  
19 tion testing, the vulnerability disclo-  
20 sure program established under sec-  
21 tion 3559B, and other means,” after  
22 “periodically”;

23 (iii) in paragraph (3)—

24 (I) in subparagraph (A)—

1 (aa) in clause (iii), by strik-  
2 ing “and” at the end;

3 (bb) in clause (iv), by add-  
4 ing “and” at the end; and

5 (cc) by adding at the end  
6 the following:

7 “(v) ensure that—

8 “(I) senior agency information  
9 security officers of component agen-  
10 cies carry out responsibilities under  
11 this subchapter, as directed by the  
12 senior agency information security of-  
13 ficer of the agency or an equivalent  
14 official; and

15 “(II) senior agency information  
16 security officers of component agen-  
17 cies report to—

18 “(aa) the senior information  
19 security officer of the agency or  
20 an equivalent official; and

21 “(bb) the Chief Information  
22 Officer of the component agency  
23 or an equivalent official;”; and

24 (iv) in paragraph (5), by inserting  
25 “and the Director of the Cybersecurity and

1                   Infrastructure Security Agency” before  
2                   “on the effectiveness”;

3                   (B) in subsection (b)—

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

6                   “(1) pursuant to subsection (a)(1)(A), per-  
7                   forming ongoing and continuous agency system risk  
8                   assessments, which may include using guidelines and  
9                   automated tools consistent with standards and  
10                  guidelines promulgated under section 11331 of title  
11                  40, as applicable;”;

12                  (ii) in paragraph (2)—

13                  (I) by striking subparagraph (B)  
14                  and inserting the following:

15                  “(B) comply with the risk-based cyber  
16                  budget model developed pursuant to section  
17                  3553(a)(7);” and

18                  (II) in subparagraph (D)—

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

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

24                  “(iii) binding operational directives  
25                  and emergency directives promulgated by

1 the Director of the Cybersecurity and In-  
2 frastructure Security Agency under section  
3 3553;” and

4 (cc) in clause (iv), as so re-  
5 designated, by striking “as deter-  
6 mined by the agency; and” and  
7 inserting “as determined by the  
8 agency, considering—

9 “(I) the agency risk assessment  
10 performed under subsection (a)(1)(A);  
11 and

12 “(II) the determinations of ap-  
13 plying more stringent standards and  
14 additional cybersecurity procedures  
15 pursuant to section 11331(c)(1) of  
16 title 40; and”;

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

20 (iv) in paragraph (6), by striking  
21 “planning, implementing, evaluating, and  
22 documenting” and inserting “planning and  
23 implementing and, in consultation with the  
24 Director of the Cybersecurity and Infra-

1 structure Security Agency, evaluating and  
2 documenting”;

3 (v) by redesignating paragraphs (7)  
4 and (8) as paragraphs (8) and (9), respec-  
5 tively;

6 (vi) by inserting after paragraph (6)  
7 the following:

8 “(7) a process for providing the status of every  
9 remedial action and known system vulnerability to  
10 the Director and the Director of the Cybersecurity  
11 and Infrastructure Security Agency, using automa-  
12 tion and machine-readable data to the greatest ex-  
13 tent practicable;” and

14 (vii) in paragraph (8)(C), as so redes-  
15 ignated—

16 (I) by striking clause (ii) and in-  
17 serting the following:

18 “(ii) notifying and consulting with the  
19 Federal information security incident cen-  
20 ter established under section 3556 pursu-  
21 ant to the requirements of section 3594;”;

22 (II) by redesignating clause (iii)  
23 as clause (iv);

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

1                   “(iii) performing the notifications and  
2                   other activities required under subchapter  
3                   IV of this title; and”; and

4                   (IV) in clause (iv), as so redesign-  
5                   nated—

6                   (aa) in subclause (I), by  
7                   striking “and relevant offices of  
8                   inspectors general”;

9                   (bb) in subclause (II), by  
10                  adding “and” at the end;

11                  (cc) by striking subclause  
12                  (III); and

13                  (dd) by redesignating sub-  
14                  clause (IV) as subclause (III);

15                  (C) in subsection (c)—

16                  (i) by redesignating paragraph (2) as  
17                  paragraph (5);

18                  (ii) by striking paragraph (1) and in-  
19                  serting the following:

20                  “(1) BIENNIAL REPORT.—Not later than 2  
21                  years after the date of enactment of the Federal In-  
22                  formation Security Modernization Act of 2021 and  
23                  not less frequently than once every 2 years there-  
24                  after, using the continuous and ongoing agency sys-  
25                  tem risk assessment under subsection (a)(1)(A), the

1 head of each agency shall submit to the Director,  
2 the Director of the Cybersecurity and Infrastructure  
3 Security Agency, the Committee on Homeland Secu-  
4 rity and Governmental Affairs of the Senate, the  
5 Committee on Oversight and Reform of the House  
6 of Representatives, the Committee on Homeland Se-  
7 curity of the House of Representatives, the appro-  
8 priate authorization and appropriations committees  
9 of Congress, the National Cyber Director, and the  
10 Comptroller General of the United States a report  
11 that—

12 “(A) summarizes the agency system risk  
13 assessment performed under subsection  
14 (a)(1)(A);

15 “(B) evaluates the adequacy and effective-  
16 ness of information security policies, proce-  
17 dures, and practices of the agency to address  
18 the risks identified in the agency system risk  
19 assessment performed under subsection  
20 (a)(1)(A), including an analysis of the agency’s  
21 cybersecurity and incident response capabilities  
22 using the metrics established under section  
23 224(c) of the Cybersecurity Act of 2015 (6  
24 U.S.C. 1522(c));

1           “(C) summarizes the evaluation and imple-  
2           mentation plans described in subparagraphs (F)  
3           and (G) of subsection (a)(1) and whether those  
4           evaluation and implementation plans call for  
5           the use of additional cybersecurity procedures  
6           determined to be appropriate by the agency;  
7           and

8           “(D) summarizes the status of remedial  
9           actions identified by inspector general of the  
10          agency, the Comptroller General of the United  
11          States, and any other source determined appro-  
12          priate by the head of the agency.

13          “(2) UNCLASSIFIED REPORTS.—Each report  
14          submitted under paragraph (1)—

15                 “(A) shall be, to the greatest extent prac-  
16                 ticable, in an unclassified and otherwise uncon-  
17                 trolled form; and

18                 “(B) may include a classified annex.

19          “(3) ACCESS TO INFORMATION.—The head of  
20          an agency shall ensure that, to the greatest extent  
21          practicable, information is included in the unclassi-  
22          fied form of the report submitted by the agency  
23          under paragraph (2)(A).

24          “(4) BRIEFINGS.—During each year during  
25          which a report is not required to be submitted under

1 paragraph (1), the Director shall provide to the con-  
2 gressional committees described in paragraph (1) a  
3 briefing summarizing current agency and Federal  
4 risk postures.”; and

5 (iii) in paragraph (5), as so redesign-  
6 nated, by inserting “including the report-  
7 ing procedures established under section  
8 11315(d) of title 40 and subsection  
9 (a)(3)(A)(v) of this section”; and

10 (D) in subsection (d)(1), in the matter pre-  
11 ceding subparagraph (A), by inserting “and the  
12 Director of the Cybersecurity and Infrastruc-  
13 ture Security Agency” after “the Director”; and  
14 (4) in section 3555—

15 (A) in the section heading, by striking  
16 “**ANNUAL INDEPENDENT**” and inserting  
17 “**INDEPENDENT**”;

18 (B) in subsection (a)—

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

23 (ii) in paragraph (2)(A), by inserting  
24 “, including by penetration testing and  
25 analyzing the vulnerability disclosure pro-

1                   gram of the agency” after “information  
2                   systems”; and

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

5           “(3) An evaluation under this section may include  
6 recommendations for improving the cybersecurity posture  
7 of the agency.”;

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

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

13                   (E) by striking subsection (f) and inserting  
14                   the following:

15           “(f) PROTECTION OF INFORMATION.—(1) Agencies,  
16 evaluators, and other recipients of information that, if dis-  
17 closed, may cause grave harm to the efforts of Federal  
18 information security officers shall take appropriate steps  
19 to ensure the protection of that information, including  
20 safeguarding the information from public disclosure.

21           “(2) The protections required under paragraph (1)  
22 shall be commensurate with the risk and comply with all  
23 applicable laws and regulations.

24           “(3) With respect to information that is not related  
25 to national security systems, agencies and evaluators shall

1 make a summary of the information unclassified and pub-  
2 licly available, including information that does not iden-  
3 tify—

4 “(A) specific information system incidents; or

5 “(B) specific information system  
6 vulnerabilities.”;

7 (F) in subsection (g)(2)—

8 (i) by striking “this subsection shall”

9 and inserting “this subsection—

10 “(A) shall”;

11 (ii) in subparagraph (A), as so des-

12 ignated, by striking the period at the end

13 and inserting “; and”; and

14 (iii) by adding at the end the fol-

15 lowing:

16 “(B) identify any entity that performs an inde-

17 pendent evaluation under subsection (b).”; and

18 (G) by striking subsection (j) and inserting

19 the following:

20 “(j) GUIDANCE.—

21 “(1) IN GENERAL.—The Director, in consulta-

22 tion with the Director of the Cybersecurity and In-

23 frastructure Security Agency, the Chief Information

24 Officers Council, the Council of the Inspectors Gen-

25 eral on Integrity and Efficiency, and other interested

1 parties as appropriate, shall ensure the development  
2 of guidance for evaluating the effectiveness of an in-  
3 formation security program and practices

4 “(2) PRIORITIES.—The guidance developed  
5 under paragraph (1) shall prioritize the identifica-  
6 tion of—

7 “(A) the most common threat patterns ex-  
8 perienceed by each agency;

9 “(B) the security controls that address the  
10 threat patterns described in subparagraph (A);  
11 and

12 “(C) any other security risks unique to the  
13 networks of each agency.”; and

14 (5) in section 3556(a)—

15 (A) in the matter preceding paragraph (1),  
16 by inserting “within the Cybersecurity and In-  
17 frastructure Security Agency” after “incident  
18 center”; and

19 (B) in paragraph (4), by striking  
20 “3554(b)” and inserting “3554(a)(1)(A)”.

21 (d) CONFORMING AMENDMENTS.—

22 (1) TABLE OF SECTIONS.—The table of sections  
23 for chapter 35 of title 44, United States Code, is  
24 amended—

1 (A) by striking the item relating to section  
2 3553 and inserting the following:

“3553. Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency.”; and

3 (B) by striking the item relating to section  
4 3555 and inserting the following:

“3555. Independent evaluation.”.

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

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

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

16 (i) by striking “annually thereafter”  
17 and inserting “thereafter during the years  
18 during which a report is required to be  
19 submitted under section 3553(c) of title  
20 44, United States Code”; and

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

1           (3)     NIST       RESPONSIBILITIES.—Section  
2     20(d)(3)(B) of the National Institute of Standards  
3     and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is  
4     amended by striking “annual”.

5     (e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

9           “SUBCHAPTER IV—FEDERAL SYSTEM  
10                            INCIDENT RESPONSE

11    **“§ 3591. Definitions**

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

15           “(b) ADDITIONAL DEFINITIONS.—As used in this  
16    subchapter:

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

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

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

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

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

3           “(E) the Committee on Homeland Security  
4 of the House of Representatives;

5           “(F) the appropriate authorization and ap-  
6 propriations committees of Congress;

7           “(G) the Director;

8           “(H) the Director of the Cybersecurity and  
9 Infrastructure Security Agency;

10          “(I) the National Cyber Director;

11          “(J) the Comptroller General of the United  
12 States; and

13          “(K) the inspector general of any impacted  
14 agency.

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

16           “(A) means a person, business, or other  
17 entity that receives a grant from, or is a party  
18 to a cooperative agreement or an other trans-  
19 action agreement with, an agency; and

20           “(B) includes any subgrantee of a person,  
21 business, or other entity described in subpara-  
22 graph (A).

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

24           “(A) a compromise of the security, con-  
25 fidentiality, or integrity of data in electronic

1 form that results in unauthorized access to, or  
2 an acquisition of, personal information; or

3 “(B) a loss of data in electronic form that  
4 results in unauthorized access to, or an acquisi-  
5 tion of, personal information.

6 “(4) CONTRACTOR.—The term ‘contractor’  
7 means—

8 “(A) a prime contractor of an agency or a  
9 subcontractor of a prime contractor of an agen-  
10 cy; and

11 “(B) any person or business that collects  
12 or maintains information, including personally  
13 identifiable information, on behalf of an agency.

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

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

24 “(7) INTELLIGENCE COMMUNITY.—The term  
25 ‘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 a senior 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 rationale for the  
21           determination that notice should be provided under  
22           subsection (a);

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

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

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

5                   “(B) may include a telephone number or a  
6                   website;

7           “(4) information on any remedy being offered  
8           by the agency;

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

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

18          “(c) DELAY OF NOTIFICATION.—

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

23                   “(A) impede a criminal investigation or a  
24                   national security activity;

25                   “(B) reveal sensitive sources and methods;

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

2 “(D) hamper security remediation actions.

3 “(2) DOCUMENTATION.—

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

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

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

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

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

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

7 “(e) EXEMPTION FROM NOTIFICATION.—

8 “(1) IN GENERAL.—The head of an agency, in  
9 consultation with the inspector general of the agen-  
10 cy, may request an exemption from the Director  
11 from complying with the notification requirements  
12 under subsection (a) if the information affected by  
13 the breach is determined by an independent evalua-  
14 tion to be unreadable, including, as appropriate, in-  
15 stances in which the information is—

16 “(A) encrypted; and

17 “(B) determined by the Director of the Cy-  
18 bersecurity and Infrastructure Security Agency  
19 to be of sufficiently low risk of exposure.

20 “(2) APPROVAL.—The Director shall determine  
21 whether to grant an exemption requested under  
22 paragraph (1) in consultation with—

23 “(A) the Director of the Cybersecurity and  
24 Infrastructure Security Agency; and

25 “(B) the Attorney General.

1           “(3) DOCUMENTATION.—Any exemption grant-  
2           ed by the Director under paragraph (1) shall be re-  
3           ported in writing to the head of the agency and the  
4           inspector general of the agency that experienced the  
5           breach and the Director of the Cybersecurity and In-  
6           frastructure Security Agency.

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

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

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

18       **“§ 3593. Congressional and Executive Branch reports**

19          “(a) INITIAL REPORT.—

20          “(1) IN GENERAL.—Not later than 72 hours  
21          after an agency has a reasonable basis to conclude  
22          that a major incident occurred, the head of the  
23          agency impacted by the major incident shall submit  
24          to the appropriate reporting entities a written report  
25          and, to the extent practicable, provide a briefing to

1 the Committee on Homeland Security and Govern-  
2 mental Affairs of the Senate, the Committee on  
3 Oversight and Reform of the House of Representa-  
4 tives, the Committee on Homeland Security of the  
5 House of Representatives, and the appropriate au-  
6 thorization and appropriations committees of Con-  
7 gress, taking into account—

8 “(A) the information known at the time of  
9 the report;

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

12 “(C) the classification level of the informa-  
13 tion contained in the report.

14 “(2) CONTENTS.—A report required under  
15 paragraph (1) shall include, in a manner that ex-  
16 cludes or otherwise reasonably protects personally  
17 identifiable information and to the extent permitted  
18 by applicable law, including privacy and statistical  
19 laws—

20 “(A) a summary of the information avail-  
21 able about the major incident, including how  
22 the major incident occurred, information indi-  
23 cating that the major incident may be a breach,  
24 and information relating to the major incident  
25 as a breach, based on information available to

1 agency officials as of the date on which the  
2 agency submits the report;

3 “(B) if applicable, a description and any  
4 associated documentation of any circumstances  
5 necessitating a delay in or exemption to notifi-  
6 cation to individuals potentially affected by the  
7 major incident under subsection (c) or (e) of  
8 section 3592; and

9 “(C) if applicable, an assessment of the  
10 impacts to the agency, the Federal Government,  
11 or the security of the United States, based on  
12 information available to agency officials on the  
13 date on which the agency submits the report.

14 “(b) SUPPLEMENTAL REPORT.—Within a reasonable  
15 amount of time, but not later than 30 days after the date  
16 on which an agency submits a written report under sub-  
17 section (a), the head of the agency shall provide to the  
18 appropriate reporting entities written updates on the  
19 major incident and, to the extent practicable, provide a  
20 briefing to the congressional committees described in sub-  
21 section (a)(1), including summaries of—

22 “(1) vulnerabilities, means by which the major  
23 incident occurred, and impacts to the agency relat-  
24 ing to the major incident;

1           “(2) any risk assessment and subsequent risk-  
2           based security implementation of the affected infor-  
3           mation system before the date on which the major  
4           incident occurred;

5           “(3) the status of compliance of the affected in-  
6           formation system with applicable security require-  
7           ments at the time of the major incident;

8           “(4) an estimate of the number of individuals  
9           potentially affected by the major incident based on  
10          information available to agency officials as of the  
11          date on which the agency provides the update;

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

16          “(6) an update to the assessment of the risk to  
17          agency operations, or to impacts on other agency or  
18          non-Federal entity operations, affected by the major  
19          incident based on information available to agency of-  
20          ficials as of the date on which the agency provides  
21          the update; and

22          “(7) the detection, response, and remediation  
23          actions of the agency, including any support pro-  
24          vided by the Cybersecurity and Infrastructure Secu-  
25          rity Agency under section 3594(d) and status up-

1 dates on the notification process described in section  
2 3592(a), including any delay or exemption described  
3 in subsection (c) or (e), respectively, of section 3592,  
4 if applicable.

5 “(c) UPDATE REPORT.—If the agency determines  
6 that there is any significant change in the understanding  
7 of the agency of the scope, scale, or consequence of a  
8 major incident for which an agency submitted a written  
9 report under subsection (a), the agency shall provide an  
10 updated report to the appropriate reporting entities that  
11 includes information relating to the change in under-  
12 standing.

13 “(d) ANNUAL REPORT.—Each agency shall submit as  
14 part of the annual report required under section  
15 3554(c)(1) of this title a description of each major inci-  
16 dent that occurred during the 1-year period preceding the  
17 date on which the report is submitted.

18 “(e) DELAY AND EXEMPTION REPORT.—

19 “(1) IN GENERAL.—The Director shall submit  
20 to the appropriate notification entities an annual re-  
21 port on all notification delays and exemptions grant-  
22 ed pursuant to subsections (c) and (d) of section  
23 3592.

24 “(2) COMPONENT OF OTHER REPORT.—The Di-  
25 rector may submit the report required under para-

1 graph (1) as a component of the annual report sub-  
2 mitted under section 3597(b).

3 “(f) REPORT DELIVERY.—Any written report re-  
4 quired to be submitted under this section may be sub-  
5 mitted in a paper or electronic format.

6 “(g) THREAT BRIEFING.—

7 “(1) IN GENERAL.—Not later than 7 days after  
8 the date on which an agency has a reasonable basis  
9 to conclude that a major incident occurred, the head  
10 of the agency, jointly with the National Cyber Direc-  
11 tor and any other Federal entity determined appro-  
12 priate by the National Cyber Director, shall provide  
13 a briefing to the congressional committees described  
14 in subsection (a)(1) on the threat causing the major  
15 incident.

16 “(2) COMPONENTS.—The briefing required  
17 under paragraph (1)—

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

20 “(B) may include a classified component.

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

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

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

4   **“§ 3594. Government information sharing and inci-**  
5           **dent response**

6           “(a) IN GENERAL.—

7           “(1) INCIDENT REPORTING.—The head of each  
8           agency shall provide any information relating to any  
9           incident, whether the information is obtained by the  
10          Federal Government directly or indirectly, to the Cy-  
11          bersecurity and Infrastructure Security Agency and  
12          the Office of Management and Budget.

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

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

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

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

1                   “(i) how the safeguards described in  
2                   subparagraph (A) should be implemented  
3                   differently; and

4                   “(ii) additional necessary safeguards;  
5                   and

6                   “(D) include information to aid in incident  
7                   response, such as—

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

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

12                   “(iii) information that could reason-  
13                   ably help identify the party that conducted  
14                   the incident.

15                   “(3) INFORMATION SHARING.—To the greatest  
16                   extent practicable, the Director of the Cybersecurity  
17                   and Infrastructure Security Agency shall share in-  
18                   formation relating to an incident with any agencies  
19                   that may be impacted by the incident.

20                   “(4) NATIONAL SECURITY SYSTEMS.—Each  
21                   agency operating or exercising control of a national  
22                   security system shall share information about inci-  
23                   dents that occur on national security systems with  
24                   the Director of the Cybersecurity and Infrastructure  
25                   Security Agency to the extent consistent with stand-

1       ards and guidelines for national security systems  
2       issued in accordance with law and as directed by the  
3       President.

4       “(b) COMPLIANCE.—The information provided under  
5       subsection (a) shall take into account the level of classi-  
6       fication of the information and any information sharing  
7       limitations and protections, such as limitations and protec-  
8       tions relating to law enforcement, national security, pri-  
9       vacy, statistical confidentiality, or other factors deter-  
10      mined by the Director

11      “(c) INCIDENT RESPONSE.—Each agency that has a  
12      reasonable basis to conclude that a major incident oc-  
13      curred involving Federal information in electronic medium  
14      or form, as defined by the Director and not involving a  
15      national security system, regardless of delays from notifi-  
16      cation granted for a major incident, shall coordinate with  
17      the Cybersecurity and Infrastructure Security Agency re-  
18      garding—

19              “(1) incident response and recovery; and

20              “(2) recommendations for mitigating future in-  
21      cidents.

22      **“§ 3595. Responsibilities of contractors and awardees**

23      “(a) NOTIFICATION.—

24              “(1) IN GENERAL.—Unless otherwise specified  
25      in a contract, grant, cooperative agreement, or an

1 other transaction agreement, any contractor or  
2 awardee of an agency shall report to the agency  
3 within the same amount of time such agency is re-  
4 quired to report an incident to the Cybersecurity  
5 and Infrastructure Security Agency, if the con-  
6 tractor or awardee has a reasonable basis to con-  
7 clude that—

8 “(A) an incident or breach has occurred  
9 with respect to Federal information collected,  
10 used, or maintained by the contractor or award-  
11 ee in connection with the contract, grant, coop-  
12 erative agreement, or other transaction agree-  
13 ment of the contractor or awardee;

14 “(B) an incident or breach has occurred  
15 with respect to a Federal information system  
16 used or operated by the contractor or awardee  
17 in connection with the contract, grant, coopera-  
18 tive agreement, or other transaction agreement  
19 of the contractor or awardee; or

20 “(C) the contractor or awardee has re-  
21 ceived information from the agency that the  
22 contractor or awardee is not authorized to re-  
23 ceive in connection with the contract, grant, co-  
24 operative agreement, or other transaction agree-  
25 ment of the contractor or awardee.

1 “(2) PROCEDURES.—

2 “(A) MAJOR INCIDENT.—Following a re-  
3 port of a breach or major incident by a con-  
4 tractor or awardee under paragraph (1), the  
5 agency, in consultation with the contractor or  
6 awardee, shall carry out the requirements under  
7 sections 3592, 3593, and 3594 with respect to  
8 the major incident.

9 “(B) INCIDENT.—Following a report of an  
10 incident by a contractor or awardee under para-  
11 graph (1), an agency, in consultation with the  
12 contractor or awardee, shall carry out the re-  
13 quirements under section 3594 with respect to  
14 the incident.

15 “(b) EFFECTIVE DATE.—This section shall apply on  
16 and after the date that is 1 year after the date of enact-  
17 ment of the Federal Information Security Modernization  
18 Act of 2021.

19 **“§ 3596. Training**

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

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

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

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

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

15       **“§ 3597. Analysis and report on Federal incidents**

16       “(a) ANALYSIS OF FEDERAL INCIDENTS.—

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

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

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

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

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

8                   “(C) cross Federal Government root causes  
9                   of incidents at agencies;

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

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

16                  “(F) trends in cross-Federal Government  
17                  cybersecurity and incident response capabilities  
18                  using the metrics established under section  
19                  224(c) of the Cybersecurity Act of 2015 (6  
20                  U.S.C. 1522(c)).

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

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

1           “(A) IN GENERAL.—The Director shall  
2 share on an ongoing basis the analyses required  
3 under this subsection with agencies and the Na-  
4 tional Cyber Director to—

5                   “(i) improve the understanding of cy-  
6 bersecurity risk of agencies; and

7                   “(ii) support the cybersecurity im-  
8 provement efforts of agencies.

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

12                   “(i) in human-readable written prod-  
13 ucts; and

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

18           “(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—  
19 Not later than 2 years after the date of enactment of this  
20 section, and not less frequently than annually thereafter,  
21 the Director of the Cybersecurity and Infrastructure Secu-  
22 rity Agency, in consultation with the Director and other  
23 Federal agencies as appropriate, shall submit to the ap-  
24 propriate notification 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                 “(B) the total number of compromises of  
16 the agency; and

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

21           “(c) PUBLICATION.—A version of each report sub-  
22 mitted under subsection (b) shall be made publicly avail-  
23 able on the website of the Cybersecurity and Infrastruc-  
24 ture Security Agency during the year in which the report  
25 is submitted.

1 “(d) INFORMATION PROVIDED BY AGENCIES.—

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

6 “(2) NONCOMPLIANCE REPORTS.—

7 “(A) IN GENERAL.—Subject to subpara-  
8 graph (B), during any year during which the  
9 head of an agency does not provide data for an  
10 incident to the Cybersecurity and Infrastructure  
11 Security Agency in accordance with section  
12 3594(a), the head of the agency, in coordina-  
13 tion with the Director of the Cybersecurity and  
14 Infrastructure Security Agency and the Direc-  
15 tor, shall submit to the appropriate reporting  
16 entities a report that includes—

17 “(i) data for the incident; and

18 “(ii) the information described in sub-  
19 section (b) with respect to the agency.

20 “(B) EXCEPTION FOR NATIONAL SECURITY  
21 SYSTEMS.—The head of an agency that owns or  
22 exercises control of a national security system  
23 shall not include data for an incident that oc-  
24 curs on a national security system in any report  
25 submitted under subparagraph (A).

1           “(3) NATIONAL SECURITY SYSTEM REPORTS.—

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

11                           “(i) the majority and minority leaders  
12 of the Senate,

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

15                           “(iii) the Committee on Homeland Se-  
16 curity and Governmental Affairs of the  
17 Senate;

18                           “(iv) the Select Committee on Intel-  
19 ligence of the Senate;

20                           “(v) the Committee on Armed Serv-  
21 ices of the Senate;

22                           “(vi) the Committee on Appropria-  
23 tions of the Senate;

24                           “(vii) the Committee on Oversight and  
25 Reform of the House of Representatives;

1 “(viii) the Committee on Homeland  
2 Security of the House of Representatives;

3 “(ix) the Permanent Select Committee  
4 on Intelligence of the House of Represent-  
5 atives;

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

8 “(xi) the Committee on Appropria-  
9 tions of the House of Representatives.

10 “(B) CLASSIFIED FORM.—A report re-  
11 quired under subparagraph (A) may be sub-  
12 mitted in a classified form.

13 “(e) REQUIREMENT FOR COMPILING INFORMA-  
14 TION.—In publishing the public report required under  
15 subsection (c), the Director of the Cybersecurity and In-  
16 frastructure Security Agency shall sufficiently compile in-  
17 formation such that no specific incident of an agency can  
18 be identified, except with the concurrence of the Director  
19 of the Office of Management and Budget and in consulta-  
20 tion with the impacted agency.

21 **“§ 3598. Major incident definition**

22 “(a) IN GENERAL.—Not later than 180 days after  
23 the date of enactment of the Federal Information Security  
24 Modernization Act of 2021, the Director, in coordination  
25 with the Director of the Cybersecurity and Infrastructure

1 Security Agency and the National Cyber Director, shall  
2 develop and promulgate guidance on the definition of the  
3 term ‘major incident’ for the purposes of subchapter II  
4 and this subchapter.

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

8 “(1) include, with respect to any information  
9 collected or maintained by or on behalf of an agency  
10 or an information system used or operated by an  
11 agency or by a contractor of an agency or another  
12 organization on behalf of an agency—

13 “(A) any incident the head of the agency  
14 determines is likely to have an impact on—

15 “(i) the national security, homeland  
16 security, or economic security of the  
17 United States; or

18 “(ii) the civil liberties or public health  
19 and safety of the people of the United  
20 States;

21 “(B) any incident the head of the agency  
22 determines likely to result in an inability for the  
23 agency, a component of the agency, or the Fed-  
24 eral Government, to provide 1 or more critical  
25 services;

1           “(C) any incident that the head of an  
2 agency, in consultation with a senior privacy of-  
3 ficer of the agency, determines is likely to have  
4 a significant privacy impact on 1 or more indi-  
5 vidual;

6           “(D) any incident that the head of the  
7 agency, in consultation with a senior privacy of-  
8 ficial of the agency, determines is likely to have  
9 a substantial privacy impact on a significant  
10 number of individuals;

11           “(E) any incident the head of the agency  
12 determines impacts the operations of a high  
13 value asset owned or operated by the agency;

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

20           “(G) any other type of incident determined  
21 appropriate by the Director;

22           “(2) stipulate that the National Cyber Director  
23 shall declare a major incident at each agency im-  
24 pacted by an incident if the Director of the Cyberse-

1 security and Infrastructure Security Agency deter-  
2 mines that an incident—

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

4 and

5 “(B) is enabled by—

6 “(i) a common technical root cause,  
7 such as a supply chain compromise, a com-  
8 mon software or hardware vulnerability; or

9 “(ii) the related activities of a com-  
10 mon threat actor; and

11 “(3) stipulate that, in determining whether an  
12 incident constitutes a major incident because that  
13 incident—

14 “(A) is any incident described in para-  
15 graph (1), the head of an agency shall consult  
16 with the Director of the Cybersecurity and In-  
17 frastructure Security Agency;

18 “(B) is an incident described in paragraph  
19 (1)(A), the head of the agency shall consult  
20 with the National Cyber Director; and

21 “(C) is an incident described in subpara-  
22 graph (C) or (D) of paragraph (1), the head of  
23 the agency shall consult with—

24 “(i) the Privacy and Civil Liberties  
25 Oversight Board; and

1                   “(ii) the Chair of the Federal Trade  
2                   Commission.

3           “(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In de-  
4           termining what constitutes a significant number of indi-  
5           viduals under subsection (b)(1)(D), the Director—

6                   “(1) may determine a threshold for a minimum  
7           number of individuals that constitutes a significant  
8           amount; and

9                   “(2) may not determine a threshold described  
10          in paragraph (1) that exceeds 5,000 individuals.

11          “(d) EVALUATION AND UPDATES.—Not later than 2  
12          years after the date of enactment of the Federal Informa-  
13          tion Security Modernization Act of 2021, and not less fre-  
14          quently than every 2 years thereafter, the Director shall  
15          submit to the Committee on Homeland Security and Gov-  
16          ernmental Affairs of the Senate and the Committee on  
17          Oversight and Reform of the House of Representatives an  
18          evaluation, which shall include—

19                   “(1) an update, if necessary, to the guidance  
20          issued under subsection (a);

21                   “(2) the definition of the term ‘major incident’  
22          included in the guidance issued under subsection (a);  
23          and

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

1           (2) CLERICAL AMENDMENT.—The table of sec-  
2           tions for chapter 35 of title 44, United States Code,  
3           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.”.

4   **SEC. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.**

5           (a) INFORMATION TECHNOLOGY MODERNIZATION  
6           CENTERS OF EXCELLENCE PROGRAM ACT.—Section  
7           2(c)(4)(A)(ii) of the Information Technology Moderniza-  
8           tion Centers of Excellence Program Act (40 U.S.C. 11301  
9           note) is amended by striking the period at the end and  
10          inserting “, which shall be provided in coordination with  
11          the Director of the Cybersecurity and Infrastructure Secu-  
12          rity Agency.”.

13          (b) MODERNIZING GOVERNMENT TECHNOLOGY.—  
14          Subtitle G of title X of Division A of the National Defense  
15          Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301  
16          note) is amended—

17                 (1) in section 1077(b)—

18                         (A) in paragraph (5)(A), by inserting “im-  
19                         proving the cybersecurity of systems and” be-  
20                         fore “cost savings activities”; and

21                         (B) in paragraph (7)—

1 (i) in the paragraph heading, by strik-  
2 ing “CIO” and inserting “CIO”;

3 (ii) by striking “In evaluating  
4 projects” and inserting the following:

5 “(A) CONSIDERATION OF GUIDANCE.—In  
6 evaluating projects”;

7 (iii) in subparagraph (A), as so des-  
8 ignated, by striking “under section  
9 1094(b)(1)” and inserting “by the Direc-  
10 tor”; and

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

13 “(B) CONSULTATION.—In using funds  
14 under paragraph (3)(A), the Chief Information  
15 Officer of the covered agency shall consult with  
16 the necessary stakeholders to ensure the project  
17 appropriately addresses cybersecurity risks, in-  
18 cluding the Director of the Cybersecurity and  
19 Infrastructure Security Agency, as appro-  
20 priate.”; and

21 (2) in section 1078—

22 (A) by striking subsection (a) and insert-  
23 ing the following:

24 “(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.”;

7           (B) in subsection (b), by adding at the end  
8 the following:

9           “(8) PROPOSAL EVALUATION.—The Director  
10 shall—

11           “(A) give consideration for the use of  
12 amounts in the Fund to improve the security of  
13 high value assets; and

14           “(B) require that any proposal for the use  
15 of amounts in the Fund includes a cybersecu-  
16 rity plan, including a supply chain risk manage-  
17 ment plan, to be reviewed by the member of the  
18 Technology Modernization Board described in  
19 subsection (c)(5)(C).”; and

20           (C) in subsection (c)—

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

25           (ii) in paragraph (5)—

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

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

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

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

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

16 (c) SUBCHAPTER I.—Subchapter I of subtitle III of  
17 title 40, United States Code, is amended—

18 (1) in section 11302—

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

25 (B) in subsection (c)—

1 (i) in paragraph (3)—  
2 (I) in subparagraph (A)—  
3 (aa) by striking “including  
4 data” and inserting “which  
5 shall—  
6 “(i) include data”;  
7 (bb) in clause (i), as so des-  
8 ignated, by striking “, and per-  
9 formance” and inserting “secu-  
10 rity, and performance; and”; and  
11 (cc) by adding at the end  
12 the following:  
13 “(ii) specifically denote cybersecurity  
14 funding under the risk-based cyber budget  
15 model developed pursuant to section  
16 3553(a)(7) of title 44.”; and  
17 (II) in subparagraph (B), adding  
18 at the end the following:  
19 “(iii) The Director shall provide to the  
20 National Cyber Director any cybersecurity  
21 funding information described in subpara-  
22 graph (A)(ii) that is provided to the Direc-  
23 tor under clause (ii) of this subpara-  
24 graph.”; and

1 (ii) in paragraph (4)(B), in the matter  
2 preceding clause (i), by inserting “not later  
3 than 30 days after the date on which the  
4 review under subparagraph (A) is com-  
5 pleted,” before “the Administrator”;

6 (C) in subsection (f)—

7 (i) by striking “heads of executive  
8 agencies to develop” and inserting “heads  
9 of executive agencies to—

10 “(1) develop”;

11 (ii) in paragraph (1), as so des-  
12 ignated, by striking the period at the end  
13 and inserting “; and”; and

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

16 “(2) consult with the Director of the Cybersecu-  
17 rity and Infrastructure Security Agency for the de-  
18 velopment and use of supply chain security best  
19 practices.”; and

20 (D) in subsection (h), by inserting “, in-  
21 cluding cybersecurity performances,” after “the  
22 performances”; and

23 (2) in section 11303(b)—

24 (A) in paragraph (2)(B)—

1 (i) in clause (i), by striking “or” at  
2 the end;

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

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

7 “(iii) whether the function should be  
8 performed by a shared service offered by  
9 another executive agency;”; and

10 (B) in paragraph (5)(B)(i), by inserting “,  
11 while taking into account the risk-based cyber  
12 budget model developed pursuant to section  
13 3553(a)(7) of title 44” after “title 31”.

14 (d) SUBCHAPTER II.—Subchapter II of subtitle III  
15 of title 40, United States Code, is amended—

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

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

21 (3) in section 11315, by adding at the end the  
22 following:

23 “(d) COMPONENT AGENCY CHIEF INFORMATION OF-  
24 FICERS.—The Chief Information Officer or an equivalent  
25 official of a component agency shall report to—

1           “(1) the Chief Information Officer designated  
2           under section 3506(a)(2) of title 44 or an equivalent  
3           official of the agency of which the component agency  
4           is a component; and

5           “(2) the head of the component agency.”;

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

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

11          (e) SUBCHAPTER III.—Section 11331 of title 40,  
12          United States Code, is amended—

13           (1) in subsection (a), by striking “section  
14          3532(b)(1)” and inserting “section 3552(b)”;

15           (2) in subsection (b)(1)(A)—

16                   (A) by striking “in consultation” and in-  
17                   serting “in coordination”; and

18                   (B) by striking “the Secretary of Home-  
19                   land Security” and inserting “the Director of  
20                   the Cybersecurity and Infrastructure Security  
21                   Agency”;

22           (3) by striking subsection (c) and inserting the  
23          following:

24          “(c) APPLICATION OF MORE STRINGENT STAND-  
25          ARDS.—

1           “(1) IN GENERAL.—The head of an agency  
2 shall—

3           “(A) evaluate, in consultation with the sen-  
4           ior agency information security officers, the  
5           need to employ standards for cost-effective,  
6           risk-based information security for all systems,  
7           operations, and assets within or under the su-  
8           pervision of the agency that are more stringent  
9           than the standards promulgated by the Director  
10          under this section, if such standards contain, at  
11          a minimum, the provisions of those applicable  
12          standards made compulsory and binding by the  
13          Director; and

14          “(B) to the greatest extent practicable and  
15          if the head of the agency determines that the  
16          standards described in subparagraph (A) are  
17          necessary, employ those standards.

18          “(2) EVALUATION OF MORE STRINGENT STAND-  
19          ARDS.—In evaluating the need to employ more strin-  
20          gent standards under paragraph (1), the head of an  
21          agency shall consider available risk information,  
22          such as—

23                 “(A) the status of cybersecurity remedial  
24                 actions of the agency;

1           “(B) any vulnerability information relating  
2 to agency systems that is known to the agency;

3           “(C) incident information of the agency;

4           “(D) information from—

5                 “(i) penetration testing performed  
6 under section 3559A of title 44; and

7                 “(ii) information from the vulner-  
8 ability disclosure program established  
9 under section 3559B of title 44;

10           “(E) agency threat hunting results under  
11 section 5145 of the Federal Information Secu-  
12 rity Modernization Act of 2021;

13           “(F) Federal and non-Federal threat intel-  
14 ligence;

15           “(G) data on compliance with standards  
16 issued under this section;

17           “(H) agency system risk assessments per-  
18 formed under section 3554(a)(1)(A) of title 44;  
19 and

20           “(I) any other information determined rel-  
21 evant by the head of the agency.”;

22 (4) in subsection (d)(2)—

23           (A) in the paragraph heading, by striking  
24 “NOTICE AND COMMENT” and inserting “CON-  
25 SULTATION, NOTICE, AND COMMENT”;

1 (B) by inserting “promulgate,” before  
2 “significantly modify”; and

3 (C) by striking “shall be made after the  
4 public is given an opportunity to comment on  
5 the Director’s proposed decision.” and inserting  
6 “shall be made—

7 “(A) for a decision to significantly modify  
8 or not promulgate such a proposed standard,  
9 after the public is given an opportunity to com-  
10 ment on the Director’s proposed decision;

11 “(B) in consultation with the Chief Infor-  
12 mation Officers Council, the Director of the Cy-  
13 bersecurity and Infrastructure Security Agency,  
14 the National Cyber Director, the Comptroller  
15 General of the United States, and the Council  
16 of the Inspectors General on Integrity and Effi-  
17 ciency;

18 “(C) considering the Federal risk assess-  
19 ments performed under section 3553(i) of title  
20 44; and

21 “(D) considering the extent to which the  
22 proposed standard reduces risk relative to the  
23 cost of implementation of the standard.”; and  
24 (5) by adding at the end the following:

1           “(e) REVIEW OF OFFICE OF MANAGEMENT AND  
2 BUDGET GUIDANCE AND POLICY.—

3           “(1) CONDUCT OF REVIEW.—

4                   “(A) IN GENERAL.—Not less frequently  
5 than once every 3 years, the Director of the Of-  
6 fice of Management and Budget, in consultation  
7 with the Chief Information Officers Council, the  
8 Director of the Cybersecurity and Infrastruc-  
9 ture Security Agency, the National Cyber Di-  
10 rector, the Comptroller General of the United  
11 States, and the Council of the Inspectors Gen-  
12 eral on Integrity and Efficiency shall review the  
13 efficacy of the guidance and policy promulgated  
14 by the Director in reducing cybersecurity risks,  
15 including an assessment of the requirements for  
16 agencies to report information to the Director,  
17 and determine whether any changes to that  
18 guidance or policy is appropriate.

19                   “(B) FEDERAL RISK ASSESSMENTS.—In  
20 conducting the review described in subpara-  
21 graph (A), the Director shall consider the Fed-  
22 eral risk assessments performed under section  
23 3553(i) of title 44.

24           “(2) UPDATED GUIDANCE.—Not later than 90  
25 days after the date on which a review is completed

1 under paragraph (1), the Director of the Office of  
2 Management and Budget shall issue updated guid-  
3 ance or policy to agencies determined appropriate by  
4 the Director, based on the results of the review.

5 “(3) PUBLIC REPORT.—Not later than 30 days  
6 after the date on which a review is completed under  
7 paragraph (1), the Director of the Office of Manage-  
8 ment and Budget shall make publicly available a re-  
9 port that includes—

10 “(A) an overview of the guidance and pol-  
11 icy promulgated under this section that is cur-  
12 rently in effect;

13 “(B) the cybersecurity risk mitigation, or  
14 other cybersecurity benefit, offered by each  
15 guidance or policy document described in sub-  
16 paragraph (A); and

17 “(C) a summary of the guidance or policy  
18 to which changes were determined appropriate  
19 during the review and what the changes are an-  
20 ticipated to include.

21 “(4) CONGRESSIONAL BRIEFING.—Not later  
22 than 30 days after the date on which a review is  
23 completed under paragraph (1), the Director shall  
24 provide to the Committee on Homeland Security and  
25 Governmental Affairs of the Senate and the Com-

1        mittee on Oversight and Reform of the House of  
2        Representatives a briefing on the review.

3        “(f) **AUTOMATED STANDARD IMPLEMENTATION**  
4 **VERIFICATION.**—When the Director of the National Insti-  
5 tute of Standards and Technology issues a proposed  
6 standard pursuant to paragraphs (2) and (3) of section  
7 20(a) of the National Institute of Standards and Tech-  
8 nology Act (15 U.S.C. 278g–3(a)), the Director of the Na-  
9 tional Institute of Standards and Technology shall con-  
10 sider developing and, if appropriate and practical, develop,  
11 in consultation with the Director of the Cybersecurity and  
12 Infrastructure Security Agency, specifications to enable  
13 the automated verification of the implementation of the  
14 controls within the standard.”.

15 **SEC. 5123. ACTIONS TO ENHANCE FEDERAL INCIDENT RE-**  
16 **SPONSE.**

17        (a) **RESPONSIBILITIES OF THE CYBERSECURITY AND**  
18 **INFRASTRUCTURE SECURITY AGENCY.**—

19            (1) **IN GENERAL.**—Not later than 180 days  
20 after the date of enactment of this Act, the Director  
21 of the Cybersecurity and Infrastructure Security  
22 Agency shall—

23            (A) develop a plan for the development of  
24 the analysis required under section 3597(a) of  
25 title 44, United States Code, as added by this

1 division, and the report required under sub-  
2 section (b) of that section that includes—

3 (i) a description of any challenges the  
4 Director anticipates encountering; and

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

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

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

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

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

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 (44 U.S.C.  
25 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) INCIDENT DATA SHARING.—

6 (A) IN GENERAL.—The Director shall de-  
7 velop guidance, to be updated not less fre-  
8 quently than once every 2 years, on the content,  
9 timeliness, and format of the information pro-  
10 vided by agencies under section 3594(a) of title  
11 44, United States Code, as added by this divi-  
12 sion.

13 (B) REQUIREMENTS.—The guidance devel-  
14 oped under subparagraph (A) shall—

15 (i) prioritize the availability of data  
16 necessary to understand and analyze—

17 (I) the causes of incidents;

18 (II) the scope and scale of inci-  
19 dents within the environments and  
20 systems of an agency;

21 (III) a root cause analysis of in-  
22 cidents that—

23 (aa) are common across the  
24 Federal Government; or

1 (bb) have a Government-  
2 wide impact;

3 (IV) agency response, recovery,  
4 and remediation actions and the effec-  
5 tiveness of those actions; and

6 (V) the impact of incidents;

7 (ii) enable the efficient development  
8 of—

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

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

17 (iii) include requirements for the time-  
18 liness of data production; and

19 (iv) include requirements for using  
20 automation and machine-readable data for  
21 data sharing and availability.

22 (3) GUIDANCE ON RESPONDING TO INFORMA-  
23 TION REQUESTS.—Not later than 1 year after the  
24 date of enactment of this Act, the Director shall de-  
25 velop guidance for agencies to implement the re-

1        requirement under section 3594(c) of title 44, United  
2        States Code, as added by this division, to provide in-  
3        formation to other agencies experiencing incidents.

4            (4) STANDARD GUIDANCE AND TEMPLATES.—  
5        Not later than 1 year after the date of enactment  
6        of this Act, the Director, in consultation with the  
7        Director of the Cybersecurity and Infrastructure Se-  
8        curity Agency, shall develop guidance and templates,  
9        to be reviewed and, if necessary, updated not less  
10       frequently than once every 2 years, for use by Fed-  
11       eral agencies in the activities required under sections  
12       3592, 3593, and 3596 of title 44, United States  
13       Code, as added by this division.

14            (5) CONTRACTOR AND AWARDEE GUIDANCE.—  
15            (A) IN GENERAL.—Not later than 1 year  
16        after the date of enactment of this Act, the Di-  
17        rector, in coordination with the Secretary of  
18        Homeland Security, the Secretary of Defense,  
19        the Administrator of General Services, and the  
20        heads of other agencies determined appropriate  
21        by the Director, shall issue guidance to Federal  
22        agencies on how to deconflict, to the greatest  
23        extent practicable, existing regulations, policies,  
24        and procedures relating to the responsibilities of  
25        contractors and awardees established under sec-

1           tion 3595 of title 44, United States Code, as  
2           added by this division.

3           (B) EXISTING PROCESSES.—To the great-  
4           est extent practicable, the guidance issued  
5           under subparagraph (A) shall allow contractors  
6           and awardees to use existing processes for noti-  
7           fying Federal agencies of incidents involving in-  
8           formation of the Federal Government.

9           (6) UPDATED BRIEFINGS.—Not less frequently  
10          than once every 2 years, the Director shall provide  
11          to the appropriate congressional committees an up-  
12          date on the guidance and templates developed under  
13          paragraphs (2) through (4).

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

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

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

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

22               “(13) to another agency in furtherance of a re-  
23               sponse to an incident (as defined in section 3552 of  
24               title 44) and pursuant to the information sharing re-  
25               quirements in section 3594 of title 44 if the head of

1 the requesting agency has made a written request to  
2 the agency that maintains the record specifying the  
3 particular portion desired and the activity for which  
4 the record is sought.”.

5 **SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA**  
6 **UPDATES.**

7 Not later than 1 year after the date of enactment  
8 of this Act, the Director, in coordination with the Director  
9 of the Cybersecurity and Infrastructure Security Agency,  
10 shall issue guidance for agencies on—

11 (1) performing the ongoing and continuous  
12 agency system risk assessment required under sec-  
13 tion 3554(a)(1)(A) of title 44, United States Code,  
14 as amended by this division;

15 (2) implementing additional cybersecurity pro-  
16 cedures, which shall include resources for shared  
17 services;

18 (3) establishing a process for providing the sta-  
19 tus of each remedial action under section 3554(b)(7)  
20 of title 44, United States Code, as amended by this  
21 division, to the Director and the Cybersecurity and  
22 Infrastructure Security Agency using automation  
23 and machine-readable data, as practicable, which  
24 shall include—

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

3 (B) templates for providing the status of  
4 the remedial action;

5 (4) interpreting the definition of “high value  
6 asset” under section 3552 of title 44, United States  
7 Code, as amended by this division; and

8 (5) a requirement to coordinate with inspectors  
9 general of agencies to ensure consistent under-  
10 standing and application of agency policies for the  
11 purpose of evaluations by inspectors general.

12 **SEC. 5125. AGENCY REQUIREMENTS TO NOTIFY PRIVATE**  
13 **SECTOR ENTITIES IMPACTED BY INCIDENTS.**

14 (a) DEFINITIONS.—In this section:

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

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

22 (b).

23 (b) GUIDANCE ON NOTIFICATION OF REPORTING EN-  
24 TITIES.—Not later than 180 days after the date of enact-  
25 ment of this Act, the Director shall issue guidance requir-

1 ing the head of each agency to notify a reporting entity  
2 of an incident that is likely to substantially affect—

3 (1) the confidentiality or integrity of sensitive  
4 information submitted by the reporting entity to the  
5 agency pursuant to a statutory or regulatory re-  
6 quirement; or

7 (2) the agency information system or systems  
8 used in the transmission or storage of the sensitive  
9 information described in paragraph (1).

10 **TITLE LII—IMPROVING**  
11 **FEDERAL CYBERSECURITY**

12 **SEC. 5141. MOBILE SECURITY STANDARDS.**

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

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

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

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

21 (1) a requirement, pursuant to section  
22 3506(b)(4) of title 44, United States Code, for every  
23 agency to maintain a continuous inventory of  
24 every—

1 (A) mobile device operated by or on behalf  
2 of the agency; and

3 (B) vulnerability identified by the agency  
4 associated with a mobile device; and

5 (2) a requirement for every agency to perform  
6 continuous evaluation of the vulnerabilities described  
7 in paragraph (1)(B) and other risks associated with  
8 the use of applications on mobile devices.

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

17 (d) BRIEFING.—Not later than 60 days after the date  
18 on which the Director issues guidance under subsection  
19 (a)(2), the Director, in coordination with the Director of  
20 the Cybersecurity and Infrastructure Security Agency,  
21 shall provide to the appropriate congressional committees  
22 a briefing on the guidance.

1 **SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT**  
2 **RESPONSE.**

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

11 (b) CONTENTS.—The recommendations provided  
12 under subsection (a) shall include—

13 (1) the types of logs to be maintained;

14 (2) the time periods to retain the logs and other  
15 relevant data;

16 (3) the time periods for agencies to enable rec-  
17 ommended logging and security requirements;

18 (4) how to ensure the confidentiality, integrity,  
19 and availability of logs;

20 (5) requirements to ensure that, upon request,  
21 in a manner that excludes or otherwise reasonably  
22 protects personally identifiable information, and to  
23 the extent permitted by applicable law (including  
24 privacy and statistical laws), agencies provide logs  
25 to—

1 (A) the Director of the Cybersecurity and  
2 Infrastructure Security Agency for a cybersecu-  
3 rity purpose; and

4 (B) the Federal Bureau of Investigation to  
5 investigate potential criminal activity; and

6 (6) requirements to ensure that, subject to com-  
7 pliance with statistical laws and other relevant data  
8 protection requirements, the highest level security  
9 operations center of each agency has visibility into  
10 all agency logs.

11 (c) GUIDANCE.—Not later than 90 days after receiv-  
12 ing the recommendations submitted under subsection (a),  
13 the Director, in consultation with the Director of the Cy-  
14 bersecurity and Infrastructure Security Agency and the  
15 Attorney General, shall, as determined to be appropriate  
16 by the Director, update guidance to agencies regarding re-  
17 quirements for logging, log retention, log management,  
18 sharing of log data with other appropriate agencies, or any  
19 other logging activity determined to be appropriate by the  
20 Director.

21 **SEC. 5143. CISA AGENCY ADVISORS.**

22 (a) IN GENERAL.—Not later than 120 days after the  
23 date of enactment of this Act, the Director of the Cyberse-  
24 curity and Infrastructure Security Agency shall assign not  
25 less than 1 cybersecurity professional employed by the Cy-

1 bersecurity and Infrastructure Security Agency to be the  
2 Cybersecurity and Infrastructure Security Agency advisor  
3 to the senior agency information security officer of each  
4 agency.

5 (b) QUALIFICATIONS.—Each advisor assigned under  
6 subsection (a) shall have knowledge of—

7 (1) cybersecurity threats facing agencies, in-  
8 cluding any specific threats to the assigned agency;

9 (2) performing risk assessments of agency sys-  
10 tems; and

11 (3) other Federal cybersecurity initiatives.

12 (c) DUTIES.—The duties of each advisor assigned  
13 under subsection (a) shall include—

14 (1) providing ongoing assistance and advice, as  
15 requested, to the agency Chief Information Officer;

16 (2) serving as an incident response point of  
17 contact between the assigned agency and the Cyber-  
18 security and Infrastructure Security Agency; and

19 (3) familiarizing themselves with agency sys-  
20 tems, processes, and procedures to better facilitate  
21 support to the agency in responding to incidents.

22 (d) LIMITATION.—An advisor assigned under sub-  
23 section (a) shall not be a contractor.

1 (e) MULTIPLE ASSIGNMENTS.—One individual advi-  
2 sor may be assigned to multiple agency Chief Information  
3 Officers under subsection (a).

4 **SEC. 5144. 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) DEFINITIONS.—In this section:

10 “(1) AGENCY OPERATIONAL PLAN.—The term  
11 ‘agency operational plan’ means a plan of an agency  
12 for the use of penetration testing.

13 “(2) RULES OF ENGAGEMENT.—The term  
14 ‘rules of engagement’ means a set of rules estab-  
15 lished by an agency for the use of penetration test-  
16 ing.

17 “(b) GUIDANCE.—

18 “(1) IN GENERAL.—The Director shall issue  
19 guidance that—

20 “(A) requires agencies to use, when and  
21 where appropriate, penetration testing on agen-  
22 cy systems; and

23 “(B) requires agencies to develop an agen-  
24 cy operational plan and rules of engagement

1 that meet the requirements under subsection  
2 (c).

3 “(2) PENETRATION TESTING GUIDANCE.—The  
4 guidance issued under this section shall—

5 “(A) permit an agency to use, for the pur-  
6 pose of performing penetration testing—

7 “(i) a shared service of the agency or  
8 another agency; or

9 “(ii) an external entity, such as a ven-  
10 dor; and

11 “(B) require agencies to provide the rules  
12 of engagement and results of penetration test-  
13 ing to the Director and the Director of the Cy-  
14 bersecurity and Infrastructure Security Agency,  
15 without regard to the status of the entity that  
16 performs the penetration testing.

17 “(c) AGENCY PLANS AND RULES OF ENGAGE-  
18 MENT.—The agency operational plan and rules of engage-  
19 ment of an agency shall—

20 “(1) require the agency to—

21 “(A) perform penetration testing on the  
22 high value assets of the agency; or

23 “(B) coordinate with the Director of the  
24 Cybersecurity and Infrastructure Security

1 Agency to ensure that penetration testing is  
2 being performed;

3 “(2) establish guidelines for avoiding, as a re-  
4 sult of penetration testing—

5 “(A) adverse impacts to the operations of  
6 the agency;

7 “(B) adverse impacts to operational envi-  
8 ronments and systems of the agency; and

9 “(C) inappropriate access to data;

10 “(3) require the results of penetration testing  
11 to include feedback to improve the cybersecurity of  
12 the agency; and

13 “(4) include mechanisms for providing consist-  
14 ently formatted, and, if applicable, automated and  
15 machine-readable, data to the Director and the Di-  
16 rector of the Cybersecurity and Infrastructure Secu-  
17 rity Agency.

18 “(d) RESPONSIBILITIES OF CISA.—The Director of  
19 the Cybersecurity and Infrastructure Security Agency  
20 shall—

21 “(1) establish a process to assess the perform-  
22 ance of penetration testing by both Federal and non-  
23 Federal entities that establishes minimum quality  
24 controls for penetration testing;

1           “(2) develop operational guidance for insti-  
2           tuting penetration testing programs at agencies;

3           “(3) develop and maintain a centralized capa-  
4           bility to offer penetration testing as a service to  
5           Federal and non-Federal entities; and

6           “(4) provide guidance to agencies on the best  
7           use of penetration testing resources.

8           “(e) RESPONSIBILITIES OF OMB.—The Director, in  
9           coordination with the Director of the Cybersecurity and  
10          Infrastructure Security Agency, shall—

11          “(1) not less frequently than annually, inven-  
12          tory all Federal penetration testing assets; and

13          “(2) develop and maintain a standardized proc-  
14          ess for the use of penetration testing.

15          “(f) PRIORITIZATION OF PENETRATION TESTING RE-  
16          SOURCES.—

17          “(1) IN GENERAL.—The Director, in coordina-  
18          tion with the Director of the Cybersecurity and In-  
19          frastructure Security Agency, shall develop a frame-  
20          work for prioritizing Federal penetration testing re-  
21          sources among agencies.

22          “(2) CONSIDERATIONS.—In developing the  
23          framework under this subsection, the Director shall  
24          consider—

1           “(A) agency system risk assessments per-  
2           formed under section 3554(a)(1)(A);

3           “(B) the Federal risk assessment per-  
4           formed under section 3553(i);

5           “(C) the analysis of Federal incident data  
6           performed under section 3597; and

7           “(D) any other information determined ap-  
8           propriate by the Director or the Director of the  
9           Cybersecurity and Infrastructure Security  
10          Agency.

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

14          “(h) DELEGATION OF AUTHORITY FOR CERTAIN  
15          SYSTEMS.—The authorities of the Director described in  
16          subsection (b) shall be delegated—

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

19                 “(2) to the Director of National Intelligence in  
20                 the case of systems described in 3553(e)(3).”.

21          (b) DEADLINE FOR GUIDANCE.—Not later than 180  
22          days after the date of enactment of this Act, the Director  
23          shall issue the guidance required under section 3559A(b)  
24          of title 44, United States Code, as added by subsection  
25          (a).

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

“3559A. Federal penetration testing.”.

5 (d) PENETRATION TESTING BY THE SECRETARY OF  
6 HOMELAND SECURITY.—Section 3553(b) of title 44,  
7 United States Code, as amended by section 5121, is fur-  
8 ther amended—

9 (1) in paragraph (8)(B), by striking “and” at  
10 the end;

11 (2) by redesignating paragraph (9) as para-  
12 graph (10); and

13 (3) by inserting after paragraph (8) the fol-  
14 lowing:

15 “(9) performing penetration testing with or  
16 without advance notice to, or authorization from,  
17 agencies, to identify vulnerabilities within Federal  
18 information systems; and”.

19 **SEC. 5145. ONGOING THREAT HUNTING PROGRAM.**

20 (a) THREAT HUNTING PROGRAM.—

21 (1) IN GENERAL.—Not later than 540 days  
22 after the date of enactment of this Act, the Director  
23 of the Cybersecurity and Infrastructure Security  
24 Agency shall establish a program to provide ongoing,

1 hypothesis-driven threat-hunting services on the net-  
2 work of each agency.

3 (2) PLAN.—Not later than 180 days after the  
4 date of enactment of this Act, the Director of the  
5 Cybersecurity and Infrastructure Security Agency  
6 shall develop a plan to establish the program re-  
7 quired under paragraph (1) that describes how the  
8 Director of the Cybersecurity and Infrastructure Se-  
9 curity Agency plans to—

10 (A) determine the method for collecting,  
11 storing, accessing, and analyzing appropriate  
12 agency data;

13 (B) provide on-premises support to agen-  
14 cies;

15 (C) staff threat hunting services;

16 (D) allocate available human and financial  
17 resources to implement the plan; and

18 (E) provide input to the heads of agencies  
19 on the use of—

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

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

1 (b) REPORTS.—The Director of the Cybersecurity  
2 and Infrastructure Security Agency shall submit to the ap-  
3 propriate congressional committees—

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

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

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

1 **SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PRO-**  
2 **GRAMS.**

3 (a) IN GENERAL.—Chapter 35 of title 44, United  
4 States Code, is amended by inserting after section 3559A,  
5 as added by section 5144 of this division, the following:

6 **“§ 3559B. Federal vulnerability disclosure programs**

7 “(a) DEFINITIONS.—In this section:

8 “(1) REPORT.—The term ‘report’ means a vul-  
9 nerability disclosure made to an agency by a re-  
10 porter.

11 “(2) REPORTER.—The term ‘reporter’ means  
12 an individual that submits a vulnerability report  
13 pursuant to the vulnerability disclosure process of an  
14 agency.

15 “(b) RESPONSIBILITIES OF OMB.—

16 “(1) LIMITATION ON LEGAL ACTION.—The Di-  
17 rector, in consultation with the Attorney General,  
18 shall issue guidance to agencies to not recommend or  
19 pursue legal action against a reporter or an indi-  
20 vidual that conducts a security research activity that  
21 the head of the agency determines—

22 “(A) represents a good faith effort to fol-  
23 low the vulnerability disclosure policy of the  
24 agency developed under subsection (d)(2); and

1           “(B) is authorized under the vulnerability  
2 disclosure policy of the agency developed under  
3 subsection (d)(2).

4           “(2) SHARING INFORMATION WITH CISA.—The  
5 Director, in coordination with the Director of the  
6 Cybersecurity and Infrastructure Security Agency  
7 and the National Cyber Director, shall issue guid-  
8 ance to agencies on sharing relevant information in  
9 a consistent, automated, and machine readable man-  
10 ner with the Cybersecurity and Infrastructure Secu-  
11 rity Agency, including—

12           “(A) any valid or credible reports of newly  
13 discovered or not publicly known vulnerabilities  
14 (including misconfigurations) on Federal infor-  
15 mation systems that use commercial software or  
16 services;

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

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

1                   “(ii) about which the head of the  
2                   agency believes the Director of the Cyber-  
3                   security and Infrastructure Security Agen-  
4                   cy should know; and

5                   “(C) any other information with respect to  
6                   which the head of the agency determines helpful  
7                   or necessary to involve the Cybersecurity and  
8                   Infrastructure Security Agency.

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

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

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

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

1           “(3) upon a request by an agency, assist the  
2 agency in the disclosure to vendors of newly identi-  
3 fied vulnerabilities in vendor products and services.

4           “(d) RESPONSIBILITIES OF AGENCIES.—

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

9                   “(A) an appropriate security contact; and

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

13           “(2) VULNERABILITY DISCLOSURE POLICY.—  
14 The head of each agency shall develop and make  
15 publicly available a vulnerability disclosure policy for  
16 the agency, which shall—

17                   “(A) describe—

18                           “(i) the scope of the systems of the  
19 agency included in the vulnerability disclo-  
20 sure policy;

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

23                           “(iii) the type of information system  
24 testing that is not authorized by the agen-  
25 cy; and

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

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

5 “(i) how the reporter should submit  
6 the report; and

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

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

13 “(D) be mature in scope, to cover all Fed-  
14 eral information systems used or operated by  
15 that agency or on behalf of that agency.

16 “(3) IDENTIFIED VULNERABILITIES.—The head  
17 of each agency shall incorporate any vulnerabilities  
18 reported under paragraph (2) into the vulnerability  
19 management process of the agency in order to track  
20 and remediate the vulnerability.

21 “(e) PAPERWORK REDUCTION ACT EXEMPTION.—  
22 The requirements of subchapter I (commonly known as  
23 the ‘Paperwork Reduction Act’) shall not apply to a vul-  
24 nerability disclosure program established under this sec-  
25 tion.

1           “(f) CONGRESSIONAL REPORTING.—Not later than  
2 90 days after the date of enactment of the Federal Infor-  
3 mation Security Modernization Act of 2021, and annually  
4 thereafter for a 3-year period, the Director shall provide  
5 to the Committee on Homeland Security and Govern-  
6 mental Affairs of the Senate and the Committee on Over-  
7 sight and Reform of the House of Representatives a brief-  
8 ing on the status of the use of vulnerability disclosure poli-  
9 cies under this section at agencies, including, with respect  
10 to the guidance issued under subsection (b)(3), an identi-  
11 fication of the agencies that are compliant and not compli-  
12 ant.

13           “(g) EXEMPTIONS.—The authorities and functions of  
14 the Director and Director of the Cybersecurity and Infra-  
15 structure Security Agency under this section shall not  
16 apply to national security systems.

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

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

23                   “(2) to the Director of National Intelligence in  
24 the case of systems described in section  
25 3553(e)(3).”.

1 (b) CLERICAL AMENDMENT.—The table of sections  
2 for chapter 35 of title 44, United States Code, is amended  
3 by adding after the item relating to section 3559A, as  
4 added by section 204, the following:

“3559B. Federal vulnerability disclosure programs.”.

5 **SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE**  
6 **AND LEAST PRIVILEGE PRINCIPLES.**

7 (a) GUIDANCE.—Not later than 1 year after the date  
8 of enactment of this Act, the Director shall provide an  
9 update to the appropriate congressional committees on  
10 progress in increasing the internal defenses of agency sys-  
11 tems, including—

12 (1) shifting away from “trusted networks” to  
13 implement security controls based on a presumption  
14 of compromise;

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

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

20 (4) identifying incidents quickly;

21 (5) isolating and removing unauthorized entities  
22 from agency systems quickly;

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

1           (7) a summary of the agency progress reports  
2           required under subsection (b).

3           (b) **AGENCY PROGRESS REPORTS.**—Not later than 1  
4           year after the date of enactment of this Act, the head of  
5           each agency shall submit to the Director a progress report  
6           on implementing an information security program based  
7           on the presumption of compromise and least privilege  
8           principles, which shall include—

9           (1) a description of any steps the agency has  
10          completed, including progress toward achieving re-  
11          quirements issued by the Director;

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

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

17 **SEC. 5148. AUTOMATION REPORTS.**

18          (a) **OMB REPORT.**—Not later than 180 days after  
19          the date of enactment of this Act, the Director shall sub-  
20          mit to the appropriate congressional committees a report  
21          on the use of automation under paragraphs (1), (5)(C)  
22          and (8)(B) of section 3554(b) of title 44, United States  
23          Code.

24          (b) **GAO REPORT.**—Not later than 1 year after the  
25          date of enactment of this Act, the Comptroller General

1 of the United States shall perform a study on the use of  
2 automation and machine readable data across the Federal  
3 Government for cybersecurity purposes, including the  
4 automated updating of cybersecurity tools, sensors, or  
5 processes by agencies.

6 **SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECUR-**  
7 **RITY COUNCIL.**

8 Section 1328 of title 41, United States Code, is  
9 amended by striking “the date that” and all that follows  
10 and inserting “December 31, 2026.”

11 **SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON IN-**  
12 **TEGRITY AND EFFICIENCY DASHBOARD.**

13 (a) DASHBOARD REQUIRED.—Section 11(e)(2) of the  
14 Inspector General Act of 1978 (5 U.S.C. App.) is amend-  
15 ed—

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

18 (2) by redesignating subparagraph (B) as sub-  
19 paragraph (C); and

20 (3) by inserting after subparagraph (A) the fol-  
21 lowing:

22 “(B) that shall include a dashboard of  
23 open information security recommendations  
24 identified in the independent evaluations re-

1           required by section 3555(a) of title 44, United  
2           States Code; and”.

3 **SEC. 5151. QUANTITATIVE CYBERSECURITY METRICS.**

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

8           (b) UPDATING AND ESTABLISHING METRICS.—Not  
9 later than 1 year after the date of enactment of this Act,  
10 the Director of the Cybersecurity and Infrastructure Secu-  
11 rity Agency, in coordination with the Director, shall—

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

14           (2) as appropriate and pursuant to section  
15 224(c) of the Cybersecurity Act of 2015 (6 U.S.C.  
16 1522(c))—

17           (A) update the covered metrics; and

18           (B) establish new covered metrics.

19           (c) IMPLEMENTATION.—

20           (1) IN GENERAL.—Not later than 540 days  
21 after the date of enactment of this Act, the Director,  
22 in coordination with the Director of the Cybersecu-  
23 rity and Infrastructure Security Agency, shall pro-  
24 mulgate guidance that requires each agency to use

1 covered metrics to track trends in the cybersecurity  
2 and incident response capabilities of the agency.

3 (2) PERFORMANCE DEMONSTRATION.—The  
4 guidance issued under paragraph (1) and any subse-  
5 quent guidance shall require agencies to share with  
6 the Director of the Cybersecurity and Infrastructure  
7 Security Agency data demonstrating the perform-  
8 ance of the agency using the covered metrics in-  
9 cluded in the guidance.

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

19 (4) ANALYSIS CAPACITY.—The Director of the  
20 Cybersecurity and Infrastructure Security Agency  
21 shall develop a capability that allows for the analysis  
22 of the covered metrics, including cross-agency per-  
23 formance of agency cybersecurity and incident re-  
24 sponse capability trends.

25 (d) CONGRESSIONAL REPORTS.—

1           (1) UTILITY OF METRICS.—Not later than 1  
2           year after the date of enactment of this Act, the Di-  
3           rector of the Cybersecurity and Infrastructure Secu-  
4           rity Agency shall submit to the appropriate congress-  
5           sional committees a report on the utility of the cov-  
6           ered metrics.

7           (2) USE OF METRICS.—Not later than 180 days  
8           after the date on which the Director promulgates  
9           guidance under subsection (c)(1), the Director shall  
10          submit to the appropriate congressional committees  
11          a report on the results of the use of the covered  
12          metrics by agencies.

13          (e) CYBERSECURITY ACT OF 2015 UPDATES.—Sec-  
14          tion 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522)  
15          is amended—

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

18               “(c) IMPROVED METRICS.—

19                       “(1) IN GENERAL.—The Director of the Cyber-  
20                       security and Infrastructure Security Agency, in co-  
21                       ordination with the Director, shall establish, review,  
22                       and update metrics to measure the cybersecurity and  
23                       incident response capabilities of agencies in accord-  
24                       ance with the responsibilities of agencies under sec-  
25                       tion 3554 of title 44, United States Code.

1           “(2) QUALITIES.—With respect to the metrics  
2 established, reviewed, and updated under paragraph  
3 (1)—

4           “(A) not less than 2 of the metrics shall be  
5 time-based, such as a metric of—

6           “(i) the amount of time it takes for  
7 an agency to detect an incident; and

8           “(ii) the amount of time that passes  
9 between—

10           “(I) the detection of an incident  
11 and the remediation of the incident;  
12 and

13           “(II) the remediation of an inci-  
14 dent and the recovery from the inci-  
15 dent; and

16           “(B) the metrics may include other meas-  
17 urable outcomes.”;

18           (2) by striking subsection (e); and

19           (3) by redesignating subsection (f) as sub-  
20 section (e).

21           **TITLE LIII—RISK-BASED**  
22           **BUDGET MODEL**

23           **SEC. 5161. DEFINITIONS.**

24           In this title:

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

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

7                   (B) the Committee on Homeland Security  
8                   and the Committee on Appropriations of the  
9                   House of Representatives.

10           (2) COVERED AGENCY.—The term “covered  
11           agency” has the meaning given the term “executive  
12           agency” in section 133 of title 41, United States  
13           Code.

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

17           (4) INFORMATION TECHNOLOGY.—The term  
18           “information technology”—

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

21                   (B) includes the hardware and software  
22                   systems of a Federal agency that monitor and  
23                   control physical equipment and processes of the  
24                   Federal agency.

1           (5) RISK-BASED BUDGET.—The term “risk-  
2 based budget” means a budget—

3           (A) developed by identifying and  
4 prioritizing cybersecurity risks and  
5 vulnerabilities, including impact on agency oper-  
6 ations in the case of a cyber attack, through  
7 analysis of threat intelligence, incident data,  
8 and tactics, techniques, procedures, and capa-  
9 bilities of cyber threats; and

10           (B) that allocates resources based on the  
11 risks identified and prioritized under subpara-  
12 graph (A).

13 **SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET**  
14 **MODEL.**

15 (a) IN GENERAL.—

16 (1) MODEL.—Not later than 1 year after the  
17 first publication of the budget submitted by the  
18 President under section 1105 of title 31, United  
19 States Code, following the date of enactment of this  
20 Act, the Director, in consultation with the Director  
21 of the Cybersecurity and Infrastructure Security  
22 Agency and the National Cyber Director and in co-  
23 ordination with the Director of the National Insti-  
24 tute of Standards and Technology, shall develop a

1 standard model for creating a risk-based budget for  
2 cybersecurity spending.

3 (2) RESPONSIBILITY OF DIRECTOR.—Section  
4 3553(a) of title 44, United States Code, as amended  
5 by section 5121 of this division, is further amended  
6 by inserting after paragraph (6) the following:

7 “(7) developing a standard risk-based budget  
8 model to inform Federal agency cybersecurity budget  
9 development; and”.

10 (3) CONTENTS OF MODEL.—The model re-  
11 quired to be developed under paragraph (1) shall—

12 (A) consider Federal and non-Federal  
13 cyber threat intelligence products, where avail-  
14 able, to identify threats, vulnerabilities, and  
15 risks;

16 (B) consider the impact of agency oper-  
17 ations of compromise of systems, including the  
18 interconnectivity to other agency systems and  
19 the operations of other agencies;

20 (C) indicate where resources should be al-  
21 located to have the greatest impact on miti-  
22 gating current and future threats and current  
23 and future cybersecurity capabilities;

24 (D) be used to inform acquisition and  
25 sustainment of—

1 (i) information technology and cyber-  
2 security tools;

3 (ii) information technology and cyber-  
4 security architectures;

5 (iii) information technology and cyber-  
6 security personnel; and

7 (iv) cybersecurity and information  
8 technology concepts of operations; and

9 (E) be used to evaluate and inform Gov-  
10 ernment-wide cybersecurity programs of the De-  
11 partment of Homeland Security.

12 (4) REQUIRED UPDATES.—Not less frequently  
13 than once every 3 years, the Director shall review,  
14 and update as necessary, the model required to be  
15 developed under this subsection.

16 (5) PUBLICATION.—The Director shall publish  
17 the model required to be developed under this sub-  
18 section, and any updates necessary under paragraph  
19 (4), on the public website of the Office of Manage-  
20 ment and Budget.

21 (6) REPORTS.—Not later than 1 year after the  
22 date of enactment of this Act, and annually there-  
23 after for each of the 2 following fiscal years or until  
24 the date on which the model required to be devel-  
25 oped under this subsection is completed, whichever is

1       sooner, the Director shall submit a report to Con-  
2       gress on the development of the model.

3       (b) REQUIRED USE OF RISK-BASED BUDGET  
4 MODEL.—

5           (1) IN GENERAL.—Not later than 2 years after  
6       the date on which the model developed under sub-  
7       section (a) is published, the head of each covered  
8       agency shall use the model to develop the annual cy-  
9       bersecurity and information technology budget re-  
10      quests of the agency.

11          (2) AGENCY PERFORMANCE PLANS.—Section  
12      3554(d)(2) of title 44, United States Code, is  
13      amended by inserting “and the risk-based budget  
14      model required under section 3553(a)(7)” after  
15      “paragraph (1)”.

16      (c) VERIFICATION.—

17          (1) IN GENERAL.—Section 1105(a)(35)(A)(i) of  
18      title 31, United States Code, is amended—

19           (A) in the matter preceding subclause (I),  
20           by striking “by agency, and by initiative area  
21           (as determined by the administration)” and in-  
22           serting “and by agency”;

23           (B) in subclause (III), by striking “and”  
24           at the end; and

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

1                   “(V) a validation that the budg-  
2                   ets submitted were developed using a  
3                   risk-based methodology; and

4                   “(VI) a report on the progress of  
5                   each agency on closing recommenda-  
6                   tions identified under the independent  
7                   evaluation required by section  
8                   3555(a)(1) of title 44.”.

9                   (2) EFFECTIVE DATE.—The amendments made  
10                  by paragraph (1) shall take effect on the date that  
11                  is 2 years after the date on which the model devel-  
12                  oped under subsection (a) is published.

13                  (d) REPORTS.—

14                  (1) INDEPENDENT EVALUATION.—Section  
15                  3555(a)(2) of title 44, United States Code, is  
16                  amended—

17                         (A) in subparagraph (B), by striking  
18                         “and” at the end;

19                         (B) in subparagraph (C), by striking the  
20                         period at the end and inserting “; and”; and

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

22                                 “(D) an assessment of how the agency im-  
23                                 plemented the risk-based budget model required  
24                                 under section 3553(a)(7) and an evaluation of

1           whether the model mitigates agency cyber  
2           vulnerabilities.”.

3           (2) ASSESSMENT.—Section 3553(c) of title 44,  
4           United States Code, as amended by section 5121, is  
5           further amended by inserting after paragraph (5)  
6           the following:

7           “(6) an assessment of—

8           “(A) Federal agency implementation of the  
9           model required under subsection (a)(7);

10           “(B) how cyber vulnerabilities of Federal  
11           agencies changed from the previous year; and

12           “(C) whether the model mitigates the  
13           cyber vulnerabilities of the Federal Govern-  
14           ment.”.

15           (e) GAO REPORT.—Not later than 3 years after the  
16           date on which the first budget of the President is sub-  
17           mitted to Congress containing the validation required  
18           under section 1105(a)(35)(A)(i)(V) of title 31, United  
19           States Code, as amended by subsection (c), the Com-  
20           ptroller General of the United States shall submit to the  
21           appropriate congressional committees a report that in-  
22           cludes—

23           (1) an evaluation of the success of covered  
24           agencies in developing risk-based budgets;

1           (2) an evaluation of the success of covered  
2 agencies in implementing risk-based budgets;

3           (3) an evaluation of whether the risk-based  
4 budgets developed by covered agencies mitigate  
5 cyber vulnerability, including the extent to which the  
6 risk-based budgets inform Federal Government-wide  
7 cybersecurity programs; and

8           (4) any other information relating to risk-based  
9 budgets the Comptroller General determines appro-  
10 priate.

11 **TITLE LIV—PILOT PROGRAMS**  
12 **TO ENHANCE FEDERAL CY-**  
13 **BERSECURITY**

14 **SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.**

15       (a) DEFINITION.—In this section, the term “active  
16 defense technique”—

17           (1) means an action taken on the systems of an  
18 entity to increase the security of information on the  
19 network of an agency by misleading an adversary;  
20 and

21           (2) includes a honeypot, deception, or purpose-  
22 fully feeding false or misleading data to an adver-  
23 sary when the adversary is on the systems of the en-  
24 tity.

1           (b) STUDY.—Not later than 180 days after the date  
2 of enactment of this Act, the Director of the Cybersecurity  
3 and Infrastructure Security Agency, in coordination with  
4 the Director, shall perform a study on the use of active  
5 defense techniques to enhance the security of agencies,  
6 which shall include—

7           (1) a review of legal restrictions on the use of  
8 different active cyber defense techniques in Federal  
9 environments, in consultation with the Department  
10 of Justice;

11           (2) an evaluation of—

12           (A) the efficacy of a selection of active de-  
13 fense techniques determined by the Director of  
14 the Cybersecurity and Infrastructure Security  
15 Agency; and

16           (B) factors that impact the efficacy of the  
17 active defense techniques evaluated under sub-  
18 paragraph (A);

19           (3) recommendations on safeguards and proce-  
20 dures that shall be established to require that active  
21 defense techniques are adequately coordinated to en-  
22 sure that active defense techniques do not impede  
23 threat response efforts, criminal investigations, and  
24 national security activities, including intelligence col-  
25 lection; and

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

3 **SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE**  
4           **PILOT.**

5           (a) **PURPOSE.**—The purpose of this section is for the  
6           Cybersecurity and Infrastructure Security Agency to run  
7           a security operation center on behalf of another agency,  
8           alleviating the need to duplicate this function at every  
9           agency, and empowering a greater centralized cybersecu-  
10          rity capability.

11          (b) **PLAN.**—Not later than 1 year after the date of  
12          enactment of this Act, the Director of the Cybersecurity  
13          and Infrastructure Security Agency shall develop a plan  
14          to establish a centralized Federal security operations cen-  
15          ter shared service offering within the Cybersecurity and  
16          Infrastructure Security Agency.

17          (c) **CONTENTS.**—The plan required under subsection  
18          (b) shall include considerations for—

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

21                 (2) staffing and resources; and

22                 (3) appropriate interagency agreements, con-  
23                 cepts of operations, and governance plans.

24          (d) **PILOT PROGRAM.**—

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

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

15 (e) BRIEFING AND REPORT.—

16           (1) BRIEFING.—Not later than 260 days after  
17 the date of enactment of this Act, the Director of  
18 the Cybersecurity and Infrastructure Security Agen-  
19 cy shall provide to the Committee on Homeland Se-  
20 curity and Governmental Affairs of the Senate and  
21 the Committee on Homeland Security and the Com-  
22 mittee on Oversight and Reform of the House of  
23 Representatives a briefing on the parameters of any  
24 1-year agreements entered into under subsection  
25 (d)(1).

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

10                           (A) the agreement; and

11                           (B) any additional agreements entered into  
12           with agencies under subsection (d).

13 **DIVISION F—CYBER INCIDENT**  
14 **REPORTING ACT OF 2021 AND**  
15 **CISA TECHNICAL CORREC-**  
16 **TIONS AND IMPROVEMENTS**  
17 **ACT OF 2021**

18 **TITLE LXI—CYBER INCIDENT**  
19 **REPORTING ACT OF 2021**

20 **SEC. 6101. SHORT TITLE.**

21           This title may be cited as the “Cyber Incident Re-  
22           porting Act of 2021”.

23 **SEC. 6102. DEFINITIONS.**

24           In this title:

1           (1) COVERED CYBER INCIDENT; COVERED ENTI-  
2           TY; CYBER INCIDENT.—The terms “covered cyber  
3           incident”, “covered entity”, and “cyber incident”  
4           have the meanings given those terms in section 2230  
5           of the Homeland Security Act of 2002, as added by  
6           section 6103 of this title.

7           (2) RANSOM PAYMENT; RANSOMWARE AT-  
8           TACK.—The terms “ransom payment” and  
9           “ransomware attack” have the meanings given those  
10          terms in section 2200 of the Homeland Security Act  
11          of 2002 (6 U.S.C. 651), as added by section 6203  
12          of this division.

13          (3) DIRECTOR.—The term “Director” means  
14          the Director of the Cybersecurity and Infrastructure  
15          Security Agency.

16          (4) INFORMATION SYSTEM; SECURITY VULNER-  
17          ABILITY.—The terms “information system” and “se-  
18          curity vulnerability” have the meanings given those  
19          terms in section 102 of the Cybersecurity Act of  
20          2015 (6 U.S.C. 1501).

21 **SEC. 6103. CYBER INCIDENT REPORTING.**

22          (a) CYBER INCIDENT REPORTING.—Title XXII of  
23          the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)  
24          is amended—

1 (1) in section 2209(b) (6 U.S.C. 659(b)), as so  
2 redesignated by section 6203(b) of this division—

3 (A) in paragraph (11), by striking “and”  
4 at the end;

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

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

8 “(13) receiving, aggregating, and analyzing re-  
9 ports related to covered cyber incidents (as defined  
10 in section 2230) submitted by covered entities (as  
11 defined in section 2230) and reports related to ran-  
12 som payments submitted by entities in furtherance  
13 of the activities specified in sections 2202(e), 2203,  
14 and 2231, this subsection, and any other authorized  
15 activity of the Director, to enhance the situational  
16 awareness of cybersecurity threats across critical in-  
17 frastructure sectors.”; and

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

19 **“Subtitle C—Cyber Incident**  
20 **Reporting**

21 **“SEC. 2230. DEFINITIONS.**

22 “In this subtitle:

23 “(1) CENTER.—The term ‘Center’ means the  
24 center established under section 2209.

1           “(2) COUNCIL.—The term ‘Council’ means the  
2           Cyber Incident Reporting Council described in sec-  
3           tion 1752(c)(1)(H) of the William M. (Mac) Thorn-  
4           berry National Defense Authorization Act for Fiscal  
5           Year 2021 (6 U.S.C. 1500(c)(1)(H)).

6           “(3) COVERED CYBER INCIDENT.—The term  
7           ‘covered cyber incident’ means a substantial cyber  
8           incident experienced by a covered entity that satis-  
9           fies the definition and criteria established by the Di-  
10          rector in the final rule issued pursuant to section  
11          2232(b).

12          “(4) COVERED ENTITY.—The term ‘covered en-  
13          tity’ means—

14                 “(A) any Federal contractor; or

15                 “(B) an entity that owns or operates crit-  
16          ical infrastructure that satisfies the definition  
17          established by the Director in the final rule  
18          issued pursuant to section 2232(b).

19          “(5) CYBER INCIDENT.—The term ‘cyber inci-  
20          dent’ has the meaning given the term ‘incident’ in  
21          section 2200.

22          “(6) CYBER THREAT.—The term ‘cyber  
23          threat’—

24                 “(A) has the meaning given the term ‘cy-  
25          bersecurity threat’ in section 2200; and

1           “(B) does not include any activity related  
2           to good faith security research, including par-  
3           ticipation in a bug-bounty program or a vulner-  
4           ability disclosure program.

5           “(7) FEDERAL CONTRACTOR.—The term ‘Fed-  
6           eral contractor’ means a business, nonprofit organi-  
7           zation, or other private sector entity that holds a  
8           Federal Government contract, unless that contractor  
9           is a party only to—

10           “(A) a service contract to provide house-  
11           keeping or custodial services; or

12           “(B) a contract to provide products or  
13           services unrelated to information technology  
14           that is below the micro-purchase threshold, as  
15           defined in section 2.101 of title 48, Code of  
16           Federal Regulations, or any successor regula-  
17           tion.

18           “(8) FEDERAL ENTITY; INFORMATION SYSTEM;  
19           SECURITY CONTROL.—The terms ‘Federal entity’,  
20           ‘information system’, and ‘security control’ have the  
21           meanings given those terms in section 102 of the  
22           Cybersecurity Act of 2015 (6 U.S.C. 1501).

23           “(9) SIGNIFICANT CYBER INCIDENT.—The term  
24           ‘significant cyber incident’ means a cybersecurity in-  
25           cident, or a group of related cybersecurity incidents,

1 that the Secretary determines is likely to result in  
2 demonstrable harm to the national security interests,  
3 foreign relations, or economy of the United States or  
4 to the public confidence, civil liberties, or public  
5 health and safety of the people of the United States.

6 “(10) SMALL ORGANIZATION.—The term ‘small  
7 organization’—

8 “(A) means—

9 “(i) a small business concern, as de-  
10 fined in section 3 of the Small Business  
11 Act (15 U.S.C. 632); or

12 “(ii) any nonprofit organization, in-  
13 cluding faith-based organizations and  
14 houses of worship, or other private sector  
15 entity with fewer than 200 employees (de-  
16 termined on a full-time equivalent basis);  
17 and

18 “(B) does not include—

19 “(i) a business, nonprofit organiza-  
20 tion, or other private sector entity that is  
21 a covered entity; or

22 “(ii) a Federal contractor.

23 **“SEC. 2231. CYBER INCIDENT REVIEW.**

24 “(a) ACTIVITIES.—The Center shall—

1           “(1) receive, aggregate, analyze, and secure,  
2           using processes consistent with the processes devel-  
3           oped pursuant to the Cybersecurity Information  
4           Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports  
5           from covered entities related to a covered cyber inci-  
6           dent to assess the effectiveness of security controls,  
7           identify tactics, techniques, and procedures adver-  
8           saries use to overcome those controls and other cy-  
9           bersecurity purposes, including to support law en-  
10          forcement investigations, to assess potential impact  
11          of incidents on public health and safety, and to have  
12          a more accurate picture of the cyber threat to crit-  
13          ical infrastructure and the people of the United  
14          States;

15          “(2) receive, aggregate, analyze, and secure re-  
16          ports to lead the identification of tactics, techniques,  
17          and procedures used to perpetuate cyber incidents  
18          and ransomware attacks;

19          “(3) coordinate and share information with ap-  
20          propriate Federal departments and agencies to iden-  
21          tify and track ransom payments, including those uti-  
22          lizing virtual currencies;

23          “(4) leverage information gathered about cyber-  
24          security incidents to—

1           “(A) enhance the quality and effectiveness  
2 of information sharing and coordination efforts  
3 with appropriate entities, including agencies,  
4 sector coordinating councils, information shar-  
5 ing and analysis organizations, technology pro-  
6 viders, critical infrastructure owners and opera-  
7 tors, cybersecurity and incident response firms,  
8 and security researchers; and

9           “(B) provide appropriate entities, including  
10 agencies, sector coordinating councils, informa-  
11 tion sharing and analysis organizations, tech-  
12 nology providers, cybersecurity and incident re-  
13 sponse firms, and security researchers, with  
14 timely, actionable, and anonymized reports of  
15 cyber incident campaigns and trends, including,  
16 to the maximum extent practicable, related con-  
17 textual information, cyber threat indicators, and  
18 defensive measures, pursuant to section 2235;

19           “(5) establish mechanisms to receive feedback  
20 from stakeholders on how the Agency can most ef-  
21 fectively receive covered cyber incident reports, ran-  
22 som payment reports, and other voluntarily provided  
23 information;

24           “(6) facilitate the timely sharing, on a vol-  
25 untary basis, between relevant critical infrastructure

1 owners and operators of information relating to cov-  
2 ered cyber incidents and ransom payments, particu-  
3 larly with respect to ongoing cyber threats or secu-  
4 rity vulnerabilities and identify and disseminate  
5 ways to prevent or mitigate similar incidents in the  
6 future;

7 “(7) for a covered cyber incident, including a  
8 ransomware attack, that also satisfies the definition  
9 of a significant cyber incident, or is part of a group  
10 of related cyber incidents that together satisfy such  
11 definition, conduct a review of the details sur-  
12 rounding the covered cyber incident or group of  
13 those incidents and identify and disseminate ways to  
14 prevent or mitigate similar incidents in the future;

15 “(8) with respect to covered cyber incident re-  
16 ports under subsection (b) involving an ongoing  
17 cyber threat or security vulnerability, immediately  
18 review those reports for cyber threat indicators that  
19 can be anonymized and disseminated, with defensive  
20 measures, to appropriate stakeholders, in coordina-  
21 tion with other divisions within the Agency, as ap-  
22 propriate;

23 “(9) publish quarterly unclassified, public re-  
24 ports that may be based on the unclassified informa-

1           tion contained in the reports required under sub-  
2           section (b);

3           “(10) proactively identify opportunities and per-  
4           form analyses, consistent with the protections in sec-  
5           tion 2235, to leverage and utilize data on  
6           ransomware attacks to support law enforcement op-  
7           erations to identify, track, and seize ransom pay-  
8           ments utilizing virtual currencies, to the greatest ex-  
9           tent practicable;

10          “(11) proactively identify opportunities, con-  
11          sistent with the protections in section 2235, to lever-  
12          age and utilize data on cyber incidents in a manner  
13          that enables and strengthens cybersecurity research  
14          carried out by academic institutions and other pri-  
15          vate sector organizations, to the greatest extent  
16          practicable;

17          “(12) on a not less frequently than annual  
18          basis, analyze public disclosures made pursuant to  
19          parts 229 and 249 of title 17, Code of Federal Reg-  
20          ulations, or any subsequent document submitted to  
21          the Securities and Exchange Commission by entities  
22          experiencing cyber incidents and compare such dis-  
23          closures to reports received by the Center; and

24          “(13) in accordance with section 2235 and sub-  
25          section (b) of this section, as soon as possible but

1 not later than 24 hours after receiving a covered  
2 cyber incident report, ransom payment report, volun-  
3 tarily submitted information pursuant to section  
4 2233, or information received pursuant to a request  
5 for information or subpoena under section 2234,  
6 make available the information to appropriate Sector  
7 Risk Management Agencies and other appropriate  
8 Federal agencies.

9 “(b) INTERAGENCY SHARING.—The Director of the  
10 Office of Management and Budget, in consultation with  
11 the Director and the National Cyber Director—

12 “(1) may establish a specific time requirement  
13 for sharing information under subsection (a)(13);  
14 and

15 “(2) shall determine the appropriate Federal  
16 agencies under subsection (a)(13).

17 “(c) PERIODIC BRIEFING.—Not later than 60 days  
18 after the effective date of the final rule required under  
19 section 2232(b), and on the first day of each month there-  
20 after, the Director, in consultation with the National  
21 Cyber Director, the Attorney General, and the Director  
22 of National Intelligence, shall provide to the majority lead-  
23 er of the Senate, the minority leader of the Senate, the  
24 Speaker of the House of Representatives, the minority  
25 leader of the House of Representatives, the Committee on

1 Homeland Security and Governmental Affairs of the Sen-  
2 ate, and the Committee on Homeland Security of the  
3 House of Representatives a briefing that characterizes the  
4 national cyber threat landscape, including the threat fac-  
5 ing Federal agencies and covered entities, and applicable  
6 intelligence and law enforcement information, covered  
7 cyber incidents, and ransomware attacks, as of the date  
8 of the briefing, which shall—

9           “(1) include the total number of reports sub-  
10       mitted under sections 2232 and 2233 during the  
11       preceding month, including a breakdown of required  
12       and voluntary reports;

13           “(2) include any identified trends in covered  
14       cyber incidents and ransomware attacks over the  
15       course of the preceding month and as compared to  
16       previous reports, including any trends related to the  
17       information collected in the reports submitted under  
18       sections 2232 and 2233, including—

19           “(A) the infrastructure, tactics, and tech-  
20       niques malicious cyber actors commonly use;  
21       and

22           “(B) intelligence gaps that have impeded,  
23       or currently are impeding, the ability to counter  
24       covered cyber incidents and ransomware  
25       threats;

1           “(3) include a summary of the known uses of  
2           the information in reports submitted under sections  
3           2232 and 2233; and

4           “(4) be unclassified, but may include a classi-  
5           fied annex.

6   **“SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER IN-**  
7           **CIDENTS.**

8           “(a) IN GENERAL.—

9           “(1) COVERED CYBER INCIDENT REPORTS.—A  
10          covered entity that is a victim of a covered cyber in-  
11          cident shall report the covered cyber incident to the  
12          Director not later than 72 hours after the covered  
13          entity reasonably believes that the covered cyber in-  
14          cident has occurred.

15          “(2) RANSOM PAYMENT REPORTS.—An entity,  
16          including a covered entity and except for an indi-  
17          vidual or a small organization, that makes a ransom  
18          payment as the result of a ransomware attack  
19          against the entity shall report the payment to the  
20          Director not later than 24 hours after the ransom  
21          payment has been made.

22          “(3) SUPPLEMENTAL REPORTS.—A covered en-  
23          tity shall promptly submit to the Director an update  
24          or supplement to a previously submitted covered  
25          cyber incident report if new or different information

1 becomes available or if the covered entity makes a  
2 ransom payment after submitting a covered cyber in-  
3 cident report required under paragraph (1).

4 “(4) PRESERVATION OF INFORMATION.—Any  
5 entity subject to requirements of paragraph (1), (2),  
6 or (3) shall preserve data relevant to the covered  
7 cyber incident or ransom payment in accordance  
8 with procedures established in the final rule issued  
9 pursuant to subsection (b).

10 “(5) EXCEPTIONS.—

11 “(A) REPORTING OF COVERED CYBER IN-  
12 CIDENT WITH RANSOM PAYMENT.—If a covered  
13 cyber incident includes a ransom payment such  
14 that the reporting requirements under para-  
15 graphs (1) and (2) apply, the covered entity  
16 may submit a single report to satisfy the re-  
17 quirements of both paragraphs in accordance  
18 with procedures established in the final rule  
19 issued pursuant to subsection (b).

20 “(B) SUBSTANTIALLY SIMILAR REPORTED  
21 INFORMATION.—The requirements under para-  
22 graphs (1), (2), and (3) shall not apply to an  
23 entity required by law, regulation, or contract  
24 to report substantially similar information to

1 another Federal agency within a substantially  
2 similar timeframe.

3 “(C) DOMAIN NAME SYSTEM.—The re-  
4 quirements under paragraphs (1), (2) and (3)  
5 shall not apply to an entity or the functions of  
6 an entity that the Director determines con-  
7 stitute critical infrastructure owned, operated,  
8 or governed by multi-stakeholder organizations  
9 that develop, implement, and enforce policies  
10 concerning the Domain Name System, such as  
11 the Internet Corporation for Assigned Names  
12 and Numbers or the Internet Assigned Num-  
13 bers Authority.

14 “(6) MANNER, TIMING, AND FORM OF RE-  
15 PORTS.—Reports made under paragraphs (1), (2),  
16 and (3) shall be made in the manner and form, and  
17 within the time period in the case of reports made  
18 under paragraph (3), prescribed in the final rule  
19 issued pursuant to subsection (b).

20 “(7) EFFECTIVE DATE.—Paragraphs (1)  
21 through (4) shall take effect on the dates prescribed  
22 in the final rule issued pursuant to subsection (b).

23 “(b) RULEMAKING.—

24 “(1) NOTICE OF PROPOSED RULEMAKING.—Not  
25 later than 2 years after the date of enactment of

1 this section, the Director, in consultation with Sector  
2 Risk Management Agencies and the heads of other  
3 Federal agencies, shall publish in the Federal Reg-  
4 ister a notice of proposed rulemaking to implement  
5 subsection (a).

6 “(2) FINAL RULE.—Not later than 18 months  
7 after publication of the notice of proposed rule-  
8 making under paragraph (1), the Director shall  
9 issue a final rule to implement subsection (a).

10 “(3) SUBSEQUENT RULEMAKINGS.—

11 “(A) IN GENERAL.—The Director may  
12 issue regulations to implement subsection (a)  
13 after issuance of the final rule under paragraph  
14 (2), including a rule to amend or revise the  
15 final rule.

16 “(B) PROCEDURES.—Any subsequent rules  
17 issued under subparagraph (A) shall comply  
18 with the requirements under chapter 5 of title  
19 5, United States Code, including the issuance of  
20 a notice of proposed rulemaking under section  
21 553 of such title.

22 “(c) ELEMENTS.—The final rule issued pursuant to  
23 subsection (b) shall be composed of the following elements:

24 “(1) A clear description of the types of entities  
25 that constitute covered entities, based on—

1           “(A) the consequences that disruption to  
2 or compromise of such an entity could cause to  
3 national security, economic security, or public  
4 health and safety;

5           “(B) the likelihood that such an entity  
6 may be targeted by a malicious cyber actor, in-  
7 cluding a foreign country; and

8           “(C) the extent to which damage, disrup-  
9 tion, or unauthorized access to such an entity,  
10 including the accessing of sensitive cybersecu-  
11 rity vulnerability information or penetration  
12 testing tools or techniques, will likely enable the  
13 disruption of the reliable operation of critical  
14 infrastructure.

15           “(2) A clear description of the types of substan-  
16 tial cyber incidents that constitute covered cyber in-  
17 cidents, which shall—

18           “(A) at a minimum, require the occurrence  
19 of—

20           “(i) the unauthorized access to an in-  
21 formation system or network with a sub-  
22 stantial loss of confidentiality, integrity, or  
23 availability of such information system or  
24 network, or a serious impact on the safety

1 and resiliency of operational systems and  
2 processes;

3 “(ii) a disruption of business or indus-  
4 trial operations due to a cyber incident; or

5 “(iii) an occurrence described in  
6 clause (i) or (ii) due to loss of service fa-  
7 cilitated through, or caused by, a com-  
8 promise of a cloud service provider, man-  
9 aged service provider, or other third-party  
10 data hosting provider or by a supply chain  
11 compromise;

12 “(B) consider—

13 “(i) the sophistication or novelty of  
14 the tactics used to perpetrate such an inci-  
15 dent, as well as the type, volume, and sen-  
16 sitivity of the data at issue;

17 “(ii) the number of individuals di-  
18 rectly or indirectly affected or potentially  
19 affected by such an incident; and

20 “(iii) potential impacts on industrial  
21 control systems, such as supervisory con-  
22 trol and data acquisition systems, distrib-  
23 uted control systems, and programmable  
24 logic controllers; and

25 “(C) exclude—

1           “(i) any event where the cyber inci-  
2           dent is perpetuated by a United States  
3           Government entity, good faith security re-  
4           search, or in response to an invitation by  
5           the owner or operator of the information  
6           system for third parties to find  
7           vulnerabilities in the information system,  
8           such as through a vulnerability disclosure  
9           program or the use of authorized penetra-  
10          tion testing services; and

11           “(ii) the threat of disruption as extor-  
12          tion, as described in section 2201(9)(A).

13           “(3) A requirement that, if a covered cyber inci-  
14          dent or a ransom payment occurs following an ex-  
15          empted threat described in paragraph (2)(C)(ii), the  
16          entity shall comply with the requirements in this  
17          subtitle in reporting the covered cyber incident or  
18          ransom payment.

19           “(4) A clear description of the specific required  
20          contents of a report pursuant to subsection (a)(1),  
21          which shall include the following information, to the  
22          extent applicable and available, with respect to a  
23          covered cyber incident:

24           “(A) A description of the covered cyber in-  
25          cident, including—

1                   “(i) identification and a description of  
2                   the function of the affected information  
3                   systems, networks, or devices that were, or  
4                   are reasonably believed to have been, af-  
5                   fected by such incident;

6                   “(ii) a description of the unauthorized  
7                   access with substantial loss of confiden-  
8                   tiality, integrity, or availability of the af-  
9                   fected information system or network or  
10                  disruption of business or industrial oper-  
11                  ations;

12                  “(iii) the estimated date range of such  
13                  incident; and

14                  “(iv) the impact to the operations of  
15                  the covered entity.

16                  “(B) Where applicable, a description of the  
17                  vulnerabilities, tactics, techniques, and proce-  
18                  dures used to perpetuate the covered cyber inci-  
19                  dent.

20                  “(C) Where applicable, any identifying or  
21                  contact information related to each actor rea-  
22                  sonably believed to be responsible for such inci-  
23                  dent.

24                  “(D) Where applicable, identification of  
25                  the category or categories of information that

1           were, or are reasonably believed to have been,  
2           accessed or acquired by an unauthorized per-  
3           son.

4           “(E) The name and other information that  
5           clearly identifies the entity impacted by the cov-  
6           ered cyber incident.

7           “(F) Contact information, such as tele-  
8           phone number or electronic mail address, that  
9           the Center may use to contact the covered enti-  
10          ty or an authorized agent of such covered enti-  
11          ty, or, where applicable, the service provider of  
12          such covered entity acting with the express per-  
13          mission of, and at the direction of, the covered  
14          entity to assist with compliance with the re-  
15          quirements of this subtitle.

16          “(5) A clear description of the specific required  
17          contents of a report pursuant to subsection (a)(2),  
18          which shall be the following information, to the ex-  
19          tent applicable and available, with respect to a ran-  
20          som payment:

21                 “(A) A description of the ransomware at-  
22                 tack, including the estimated date range of the  
23                 attack.

24                 “(B) Where applicable, a description of the  
25                 vulnerabilities, tactics, techniques, and proce-

1           dures used to perpetuate the ransomware at-  
2           tack.

3           “(C) Where applicable, any identifying or  
4           contact information related to the actor or ac-  
5           tors reasonably believed to be responsible for  
6           the ransomware attack.

7           “(D) The name and other information that  
8           clearly identifies the entity that made the ran-  
9           som payment.

10          “(E) Contact information, such as tele-  
11          phone number or electronic mail address, that  
12          the Center may use to contact the entity that  
13          made the ransom payment or an authorized  
14          agent of such covered entity, or, where applica-  
15          ble, the service provider of such covered entity  
16          acting with the express permission of, and at  
17          the direction of, that entity to assist with com-  
18          pliance with the requirements of this subtitle.

19          “(F) The date of the ransom payment.

20          “(G) The ransom payment demand, includ-  
21          ing the type of virtual currency or other com-  
22          modity requested, if applicable.

23          “(H) The ransom payment instructions,  
24          including information regarding where to send  
25          the payment, such as the virtual currency ad-

1           dress or physical address the funds were re-  
2           quested to be sent to, if applicable.

3           “(I) The amount of the ransom payment.

4           “(6) A clear description of the types of data re-  
5           quired to be preserved pursuant to subsection (a)(4)  
6           and the period of time for which the data is required  
7           to be preserved.

8           “(7) Deadlines for submitting reports to the Di-  
9           rector required under subsection (a)(3), which  
10          shall—

11           “(A) be established by the Director in con-  
12          sultation with the Council;

13           “(B) consider any existing regulatory re-  
14          porting requirements similar in scope, purpose,  
15          and timing to the reporting requirements to  
16          which such a covered entity may also be sub-  
17          ject, and make efforts to harmonize the timing  
18          and contents of any such reports to the max-  
19          imum extent practicable; and

20           “(C) balance the need for situational  
21          awareness with the ability of the covered entity  
22          to conduct incident response and investigations.

23          “(8) Procedures for—

24           “(A) entities to submit reports required by  
25          paragraphs (1), (2), and (3) of subsection (a),

1 including the manner and form thereof, which  
2 shall include, at a minimum, a concise, user-  
3 friendly web-based form;

4 “(B) the Agency to carry out the enforce-  
5 ment provisions of section 2233, including with  
6 respect to the issuance, service, withdrawal, and  
7 enforcement of subpoenas, appeals and due  
8 process procedures, the suspension and debar-  
9 ment provisions in section 2234(c), and other  
10 aspects of noncompliance;

11 “(C) implementing the exceptions provided  
12 in subparagraphs (A), (B), and (D) of sub-  
13 section (a)(5); and

14 “(D) protecting privacy and civil liberties  
15 consistent with processes adopted pursuant to  
16 section 105(b) of the Cybersecurity Act of 2015  
17 (6 U.S.C. 1504(b)) and anonymizing and safe-  
18 guarding, or no longer retaining, information  
19 received and disclosed through covered cyber in-  
20 cident reports and ransom payment reports that  
21 is known to be personal information of a spe-  
22 cific individual or information that identifies a  
23 specific individual that is not directly related to  
24 a cybersecurity threat.

1           “(9) A clear description of the types of entities  
2           that constitute other private sector entities for pur-  
3           poses of section 2230(b)(7).

4           “(d) THIRD PARTY REPORT SUBMISSION AND RAN-  
5           SOM PAYMENT.—

6           “(1) REPORT SUBMISSION.—An entity, includ-  
7           ing a covered entity, that is required to submit a  
8           covered cyber incident report or a ransom payment  
9           report may use a third party, such as an incident re-  
10          sponse company, insurance provider, service pro-  
11          vider, information sharing and analysis organization,  
12          or law firm, to submit the required report under  
13          subsection (a).

14          “(2) RANSOM PAYMENT.—If an entity impacted  
15          by a ransomware attack uses a third party to make  
16          a ransom payment, the third party shall not be re-  
17          quired to submit a ransom payment report for itself  
18          under subsection (a)(2).

19          “(3) DUTY TO REPORT.—Third-party reporting  
20          under this subparagraph does not relieve a covered  
21          entity or an entity that makes a ransom payment  
22          from the duty to comply with the requirements for  
23          covered cyber incident report or ransom payment re-  
24          port submission.

1           “(4) RESPONSIBILITY TO ADVISE.—Any third  
2 party used by an entity that knowingly makes a ran-  
3 som payment on behalf of an entity impacted by a  
4 ransomware attack shall advise the impacted entity  
5 of the responsibilities of the impacted entity regard-  
6 ing reporting ransom payments under this section.

7           “(e) OUTREACH TO COVERED ENTITIES.—

8           “(1) IN GENERAL.—The Director shall conduct  
9 an outreach and education campaign to inform likely  
10 covered entities, entities that offer or advertise as a  
11 service to customers to make or facilitate ransom  
12 payments on behalf of entities impacted by  
13 ransomware attacks, potential ransomware attack  
14 victims, and other appropriate entities of the re-  
15 quirements of paragraphs (1), (2), and (3) of sub-  
16 section (a).

17           “(2) ELEMENTS.—The outreach and education  
18 campaign under paragraph (1) shall include the fol-  
19 lowing:

20           “(A) An overview of the final rule issued  
21 pursuant to subsection (b).

22           “(B) An overview of mechanisms to submit  
23 to the Center covered cyber incident reports  
24 and information relating to the disclosure, re-

1           tention, and use of incident reports under this  
2           section.

3           “(C) An overview of the protections af-  
4           forded to covered entities for complying with  
5           the requirements under paragraphs (1), (2),  
6           and (3) of subsection (a).

7           “(D) An overview of the steps taken under  
8           section 2234 when a covered entity is not in  
9           compliance with the reporting requirements  
10          under subsection (a).

11          “(E) Specific outreach to cybersecurity  
12          vendors, incident response providers, cybersecu-  
13          rity insurance entities, and other entities that  
14          may support covered entities or ransomware at-  
15          tack victims.

16          “(F) An overview of the privacy and civil  
17          liberties requirements in this subtitle.

18          “(3) COORDINATION.—In conducting the out-  
19          reach and education campaign required under para-  
20          graph (1), the Director may coordinate with—

21                 “(A) the Critical Infrastructure Partner-  
22                 ship Advisory Council established under section  
23                 871;

24                 “(B) information sharing and analysis or-  
25                 ganizations;

1 “(C) trade associations;

2 “(D) information sharing and analysis cen-  
3 ters;

4 “(E) sector coordinating councils; and

5 “(F) any other entity as determined appro-  
6 priate by the Director.

7 “(f) ORGANIZATION OF REPORTS.—Notwithstanding  
8 chapter 35 of title 44, United States Code (commonly  
9 known as the ‘Paperwork Reduction Act’), the Director  
10 may request information within the scope of the final rule  
11 issued under subsection (b) by the alteration of existing  
12 questions or response fields and the reorganization and  
13 reformatting of the means by which covered cyber incident  
14 reports, ransom payment reports, and any voluntarily of-  
15 fered information is submitted to the Center.

16 **“SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER IN-**  
17 **CIDENTS.**

18 “(a) IN GENERAL.—Entities may voluntarily report  
19 incidents or ransom payments to the Director that are not  
20 required under paragraph (1), (2), or (3) of section  
21 2232(a), but may enhance the situational awareness of  
22 cyber threats.

23 “(b) VOLUNTARY PROVISION OF ADDITIONAL INFOR-  
24 MATION IN REQUIRED REPORTS.—Entities may volun-  
25 tarily include in reports required under paragraph (1), (2),

1 or (3) of section 2232(a) information that is not required  
2 to be included, but may enhance the situational awareness  
3 of cyber threats.

4 “(c) APPLICATION OF PROTECTIONS.—The protec-  
5 tions under section 2235 applicable to covered cyber inci-  
6 dent reports shall apply in the same manner and to the  
7 same extent to reports and information submitted under  
8 subsections (a) and (b).

9 **“SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.**

10 “(a) PURPOSE.—In the event that an entity that is  
11 required to submit a report under section 2232(a) fails  
12 to comply with the requirement to report, the Director  
13 may obtain information about the incident or ransom pay-  
14 ment by engaging the entity directly to request informa-  
15 tion about the incident or ransom payment, and if the Di-  
16 rector is unable to obtain information through such en-  
17 gagement, by issuing a subpoena to the entity, pursuant  
18 to subsection (c), to gather information sufficient to deter-  
19 mine whether a covered cyber incident or ransom payment  
20 has occurred, and, if so, whether additional action is war-  
21 ranted pursuant to subsection (d).

22 “(b) INITIAL REQUEST FOR INFORMATION.—

23 “(1) IN GENERAL.—If the Director has reason  
24 to believe, whether through public reporting or other  
25 information in the possession of the Federal Govern-

1       ment, including through analysis performed pursu-  
2       ant to paragraph (1) or (2) of section 2231(a), that  
3       an entity has experienced a covered cyber incident or  
4       made a ransom payment but failed to report such  
5       incident or payment to the Center within 72 hours  
6       in accordance with section 2232(a), the Director  
7       shall request additional information from the entity  
8       to confirm whether or not a covered cyber incident  
9       or ransom payment has occurred.

10           “(2) TREATMENT.—Information provided to the  
11       Center in response to a request under paragraph (1)  
12       shall be treated as if it was submitted through the  
13       reporting procedures established in section 2232.

14           “(c) AUTHORITY TO ISSUE SUBPOENAS AND  
15       DEBAR.—

16           “(1) IN GENERAL.—If, after the date that is 72  
17       hours from the date on which the Director made the  
18       request for information in subsection (b), the Direc-  
19       tor has received no response from the entity from  
20       which such information was requested, or received  
21       an inadequate response, the Director may issue to  
22       such entity a subpoena to compel disclosure of infor-  
23       mation the Director deems necessary to determine  
24       whether a covered cyber incident or ransom payment  
25       has occurred and obtain the information required to

1 be reported pursuant to section 2232 and any imple-  
2 menting regulations.

3 “(2) CIVIL ACTION.—

4 “(A) IN GENERAL.—If an entity fails to  
5 comply with a subpoena, the Director may refer  
6 the matter to the Attorney General to bring a  
7 civil action in a district court of the United  
8 States to enforce such subpoena.

9 “(B) VENUE.—An action under this para-  
10 graph may be brought in the judicial district in  
11 which the entity against which the action is  
12 brought resides, is found, or does business.

13 “(C) CONTEMPT OF COURT.—A court may  
14 punish a failure to comply with a subpoena  
15 issued under this subsection as contempt of  
16 court.

17 “(3) NON-DELEGATION.—The authority of the  
18 Director to issue a subpoena under this subsection  
19 may not be delegated.

20 “(4) DEBARMENT OF FEDERAL CONTRAC-  
21 TORS.—If a covered entity with a Federal Govern-  
22 ment contract, grant, cooperative agreement, or  
23 other transaction agreement fails to comply with a  
24 subpoena issued under this subsection—

1           “(A) the Director may refer the matter to  
2           the Administrator of General Services; and

3           “(B) upon receiving a referral from the Di-  
4           rector, the Administrator of General Services  
5           may impose additional available penalties, in-  
6           cluding suspension or debarment.

7           “(d) ACTIONS BY ATTORNEY GENERAL AND REGU-  
8           LATORS.—

9           “(1) IN GENERAL.—Notwithstanding section  
10          2235(a) and subsection (b)(2) of this section, if the  
11          Attorney General or the appropriate regulator deter-  
12          mines, based on information provided in response to  
13          a subpoena issued pursuant to subsection (c), that  
14          the facts relating to the covered cyber incident or  
15          ransom payment at issue may constitute grounds for  
16          a regulatory enforcement action or criminal prosecu-  
17          tion, the Attorney General or the appropriate regu-  
18          lator may use that information for a regulatory en-  
19          forcement action or criminal prosecution.

20          “(2) APPLICATION TO CERTAIN ENTITIES AND  
21          THIRD PARTIES.—A covered cyber incident or ran-  
22          som payment report submitted to the Center by an  
23          entity that makes a ransom payment or third party  
24          under section 2232 shall not be used by any Fed-  
25          eral, State, Tribal, or local government to investigate

1 or take another law enforcement action against the  
2 entity that makes a ransom payment or third party.

3 “(3) RULE OF CONSTRUCTION.—Nothing in  
4 this subtitle shall be construed to provide an entity  
5 that submits a covered cyber incident report or ran-  
6 som payment report under section 2232 any immu-  
7 nity from law enforcement action for making a ran-  
8 som payment otherwise prohibited by law.

9 “(e) CONSIDERATIONS.—When determining whether  
10 to exercise the authorities provided under this section, the  
11 Director shall take into consideration—

12 “(1) the size and complexity of the entity;

13 “(2) the complexity in determining if a covered  
14 cyber incident has occurred; and

15 “(3) prior interaction with the Agency or  
16 awareness of the entity of the policies and proce-  
17 dures of the Agency for reporting covered cyber inci-  
18 dents and ransom payments.

19 “(f) EXCLUSIONS.—This section shall not apply to a  
20 State, local, Tribal, or territorial government entity.

21 “(g) REPORT TO CONGRESS.—The Director shall  
22 submit to Congress an annual report on the number of  
23 times the Director—

24 “(1) issued an initial request for information  
25 pursuant to subsection (b);

1           “(2) issued a subpoena pursuant to subsection  
2           (c);

3           “(3) brought a civil action pursuant to sub-  
4           section (c)(2); or

5           “(4) conducted additional actions pursuant to  
6           subsection (d).

7   **“SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO**  
8           **THE FEDERAL GOVERNMENT.**

9           “(a) DISCLOSURE, RETENTION, AND USE.—

10           “(1) AUTHORIZED ACTIVITIES.—Information  
11           provided to the Center or Agency pursuant to sec-  
12           tion 2232 may be disclosed to, retained by, and used  
13           by, consistent with otherwise applicable provisions of  
14           Federal law, any Federal agency or department,  
15           component, officer, employee, or agent of the Fed-  
16           eral Government solely for—

17                   “(A) a cybersecurity purpose;

18                   “(B) the purpose of identifying—

19                           “(i) a cyber threat, including the  
20                           source of the cyber threat; or

21                           “(ii) a security vulnerability;

22                   “(C) the purpose of responding to, or oth-  
23                   erwise preventing or mitigating, a specific  
24                   threat of death, a specific threat of serious bod-  
25                   ily harm, or a specific threat of serious eco-

1            nomic harm, including a terrorist act or use of  
2            a weapon of mass destruction;

3            “(D) the purpose of responding to, inves-  
4            tigating, prosecuting, or otherwise preventing or  
5            mitigating, a serious threat to a minor, includ-  
6            ing sexual exploitation and threats to physical  
7            safety; or

8            “(E) the purpose of preventing, inves-  
9            tigating, disrupting, or prosecuting an offense  
10           arising out of a covered cyber incident or any  
11           of the offenses listed in section 105(d)(5)(A)(v)  
12           of the Cybersecurity Act of 2015 (6 U.S.C.  
13           1504(d)(5)(A)(v)).

14           “(2) AGENCY ACTIONS AFTER RECEIPT.—

15           “(A) RAPID, CONFIDENTIAL SHARING OF  
16           CYBER THREAT INDICATORS.—Upon receiving a  
17           covered cyber incident or ransom payment re-  
18           port submitted pursuant to this section, the  
19           center shall immediately review the report to  
20           determine whether the incident that is the sub-  
21           ject of the report is connected to an ongoing  
22           cyber threat or security vulnerability and where  
23           applicable, use such report to identify, develop,  
24           and rapidly disseminate to appropriate stake-

1 holders actionable, anonymized cyber threat in-  
2 dicators and defensive measures.

3 “(B) STANDARDS FOR SHARING SECURITY  
4 VULNERABILITIES.—With respect to informa-  
5 tion in a covered cyber incident or ransom pay-  
6 ment report regarding a security vulnerability  
7 referred to in paragraph (1)(B)(ii), the Director  
8 shall develop principles that govern the timing  
9 and manner in which information relating to se-  
10 curity vulnerabilities may be shared, consistent  
11 with common industry best practices and  
12 United States and international standards.

13 “(3) PRIVACY AND CIVIL LIBERTIES.—Informa-  
14 tion contained in covered cyber incident and ransom  
15 payment reports submitted to the Center or the  
16 Agency pursuant to section 2232 shall be retained,  
17 used, and disseminated, where permissible and ap-  
18 propriate, by the Federal Government in accordance  
19 with processes to be developed for the protection of  
20 personal information consistent with processes  
21 adopted pursuant to section 105 of the Cybersecu-  
22 rity Act of 2015 (6 U.S.C. 1504) and in a manner  
23 that protects from unauthorized use or disclosure  
24 any information that may contain—

1           “(A) personal information of a specific in-  
2           dividual; or

3           “(B) information that identifies a specific  
4           individual that is not directly related to a cyber-  
5           security threat.

6           “(4) DIGITAL SECURITY.—The Center and the  
7           Agency shall ensure that reports submitted to the  
8           Center or the Agency pursuant to section 2232, and  
9           any information contained in those reports, are col-  
10          lected, stored, and protected at a minimum in ac-  
11          cordance with the requirements for moderate impact  
12          Federal information systems, as described in Federal  
13          Information Processing Standards Publication 199,  
14          or any successor document.

15          “(5) PROHIBITION ON USE OF INFORMATION IN  
16          REGULATORY ACTIONS.—A Federal, State, local, or  
17          Tribal government shall not use information about a  
18          covered cyber incident or ransom payment obtained  
19          solely through reporting directly to the Center or the  
20          Agency in accordance with this subtitle to regulate,  
21          including through an enforcement action, the lawful  
22          activities of the covered entity or entity that made  
23          a ransom payment.

24          “(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—  
25          The submission of a report to the Center or the Agency

1 under section 2232 shall not constitute a waiver of any  
2 applicable privilege or protection provided by law, includ-  
3 ing trade secret protection and attorney-client privilege.

4 “(c) EXEMPTION FROM DISCLOSURE.—Information  
5 contained in a report submitted to the Office under section  
6 2232 shall be exempt from disclosure under section  
7 552(b)(3)(B) of title 5, United States Code (commonly  
8 known as the ‘Freedom of Information Act’) and any  
9 State, Tribal, or local provision of law requiring disclosure  
10 of information or records.

11 “(d) EX PARTE COMMUNICATIONS.—The submission  
12 of a report to the Agency under section 2232 shall not  
13 be subject to a rule of any Federal agency or department  
14 or any judicial doctrine regarding ex parte communica-  
15 tions with a decision-making official.

16 “(e) LIABILITY PROTECTIONS.—

17 “(1) IN GENERAL.—No cause of action shall lie  
18 or be maintained in any court by any person or enti-  
19 ty and any such action shall be promptly dismissed  
20 for the submission of a report pursuant to section  
21 2232(a) that is submitted in conformance with this  
22 subtitle and the rule promulgated under section  
23 2232(b), except that this subsection shall not apply  
24 with regard to an action by the Federal Government  
25 pursuant to section 2234(c)(2).

1           “(2) SCOPE.—The liability protections provided  
2           in subsection (e) shall only apply to or affect litiga-  
3           tion that is solely based on the submission of a cov-  
4           ered cyber incident report or ransom payment report  
5           to the Center or the Agency.

6           “(3) RESTRICTIONS.—Notwithstanding para-  
7           graph (2), no report submitted to the Agency pursu-  
8           ant to this subtitle or any communication, document,  
9           material, or other record, created for the sole pur-  
10          pose of preparing, drafting, or submitting such re-  
11          port, may be received in evidence, subject to dis-  
12          covery, or otherwise used in any trial, hearing, or  
13          other proceeding in or before any court, regulatory  
14          body, or other authority of the United States, a  
15          State, or a political subdivision thereof, provided  
16          that nothing in this subtitle shall create a defense to  
17          discovery or otherwise affect the discovery of any  
18          communication, document, material, or other record  
19          not created for the sole purpose of preparing, draft-  
20          ing, or submitting such report.

21          “(f) SHARING WITH NON-FEDERAL ENTITIES.—The  
22          Agency shall anonymize the victim who reported the infor-  
23          mation when making information provided in reports re-  
24          ceived under section 2232 available to critical infrastruc-  
25          ture owners and operators and the general public.

1       “(g) PROPRIETARY INFORMATION.—Information  
2 contained in a report submitted to the Agency under sec-  
3 tion 2232 shall be considered the commercial, financial,  
4 and proprietary information of the covered entity when so  
5 designated by the covered entity.

6       “(h) STORED COMMUNICATIONS ACT.—Nothing in  
7 this subtitle shall be construed to permit or require disclo-  
8 sure by a provider of a remote computing service or a pro-  
9 vider of an electronic communication service to the public  
10 of information not otherwise permitted or required to be  
11 disclosed under chapter 121 of title 18, United States  
12 Code (commonly known as the ‘Stored Communications  
13 Act’).”

14       (b) TECHNICAL AND CONFORMING AMENDMENT.—  
15 The table of contents in section 1(b) of the Homeland Se-  
16 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)  
17 is amended by inserting after the items relating to subtitle  
18 B of title XXII the following:

“Subtitle C—Cyber Incident Reporting

“Sec. 2230. Definitions.

“Sec. 2231. Cyber Incident Review.

“Sec. 2232. Required reporting of certain cyber incidents.

“Sec. 2233. Voluntary reporting of other cyber incidents.

“Sec. 2234. Noncompliance with required reporting.

“Sec. 2235. Information shared with or provided to the Federal Government.”

19 **SEC. 6104. FEDERAL SHARING OF INCIDENT REPORTS.**

20       (a) CYBER INCIDENT REPORTING SHARING.—

21               (1) IN GENERAL.—Notwithstanding any other  
22 provision of law or regulation, any Federal agency

1 that receives a report from an entity of a cyber inci-  
2 dent, including a ransomware attack, shall provide  
3 the report to the Director as soon as possible, but  
4 not later than 24 hours after receiving the report,  
5 unless a shorter period is required by an agreement  
6 made between the Cybersecurity Infrastructure Se-  
7 curity Agency and the recipient Federal agency.

8 (2) RULE OF CONSTRUCTION.—The require-  
9 ments described in paragraph (1) shall not be con-  
10 strued to be a violation of any provision of law or  
11 policy that would otherwise prohibit disclosure with-  
12 in the executive branch.

13 (3) PROTECTION OF INFORMATION.—The Di-  
14 rector shall comply with any obligations of the re-  
15 cipient Federal agency described in paragraph (1) to  
16 protect information, including with respect to pri-  
17 vacy, confidentiality, or information security, if those  
18 obligations would impose greater protection require-  
19 ments than this Act or the amendments made by  
20 this Act.

21 (4) FOIA EXEMPTION.—Any report received by  
22 the Director pursuant to paragraph (1) shall be ex-  
23 empt from disclosure under section 552(b)(3) of title  
24 5, United States Code (commonly known as the  
25 “Freedom of Information Act”).

1           (b) CREATION OF COUNCIL.—Section 1752(c) of the  
2 William M. (Mac) Thornberry National Defense Author-  
3 ization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is  
4 amended—

5           (1) in paragraph (1)—

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

8           (B) by redesignating subparagraph (H) as  
9 subparagraph (I); and

10           (C) by inserting after subparagraph (G)  
11 the following:

12           “(H) lead an intergovernmental Cyber In-  
13 cident Reporting Council, in coordination with  
14 the Director of the Office of Management and  
15 Budget and the Director of the Cybersecurity  
16 and Infrastructure Security Agency and in con-  
17 sultation with Sector Risk Management Agen-  
18 cies (as defined in section 2201 of the Home-  
19 land Security Act of 2002 (6 U.S.C. 651)) and  
20 other appropriate Federal agencies, to coordi-  
21 nate, deconflict, and harmonize Federal incident  
22 reporting requirements, including those issued  
23 through regulations, for covered entities (as de-  
24 fined in section 2230 of such Act) and entities

1           that make a ransom payment (as defined in  
2           such section 2201 (6 U.S.C. 651)); and”; and  
3           (2) by adding at the end the following:

4           “(3) RULE OF CONSTRUCTION.—Nothing in  
5           paragraph (1)(H) shall be construed to provide any  
6           additional regulatory authority to any Federal enti-  
7           ty.”.

8           (c) HARMONIZING REPORTING REQUIREMENTS.—  
9           The National Cyber Director shall, in consultation with  
10          the Director, the Cyber Incident Reporting Council de-  
11          scribed in section 1752(c)(1)(H) of the William M. (Mac)  
12          Thornberry National Defense Authorization Act for Fiscal  
13          Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of  
14          the Office of Management and Budget, to the maximum  
15          extent practicable—

16               (1) periodically review existing regulatory re-  
17               quirements, including the information required in  
18               such reports, to report cyber incidents and ensure  
19               that any such reporting requirements and proce-  
20               dures avoid conflicting, duplicative, or burdensome  
21               requirements; and

22               (2) coordinate with the Director and regulatory  
23               authorities that receive reports relating to cyber inci-  
24               dents to identify opportunities to streamline report-  
25               ing processes, and where feasible, facilitate inter-

1 agency agreements between such authorities to per-  
2 mit the sharing of such reports, consistent with ap-  
3 plicable law and policy, without impacting the ability  
4 of such agencies to gain timely situational awareness  
5 of a covered cyber incident or ransom payment.

6 **SEC. 6105. RANSOMWARE VULNERABILITY WARNING PILOT**  
7 **PROGRAM.**

8 (a) PROGRAM.—Not later than 1 year after the date  
9 of enactment of this Act, the Director shall establish a  
10 ransomware vulnerability warning program to leverage ex-  
11 isting authorities and technology to specifically develop  
12 processes and procedures for, and to dedicate resources  
13 to, identifying information systems that contain security  
14 vulnerabilities associated with common ransomware at-  
15 tacks, and to notify the owners of those vulnerable systems  
16 of their security vulnerability.

17 (b) IDENTIFICATION OF VULNERABLE SYSTEMS.—  
18 The pilot program established under subsection (a) shall—

19 (1) identify the most common security  
20 vulnerabilities utilized in ransomware attacks and  
21 mitigation techniques; and

22 (2) utilize existing authorities to identify Fed-  
23 eral and other relevant information systems that  
24 contain the security vulnerabilities identified in para-  
25 graph (1).

1 (c) ENTITY NOTIFICATION.—

2 (1) IDENTIFICATION.—If the Director is able to  
3 identify the entity at risk that owns or operates a  
4 vulnerable information system identified in sub-  
5 section (b), the Director may notify the owner of the  
6 information system.

7 (2) NO IDENTIFICATION.—If the Director is not  
8 able to identify the entity at risk that owns or oper-  
9 ates a vulnerable information system identified in  
10 subsection (b), the Director may utilize the subpoena  
11 authority pursuant to section 2209 of the Homeland  
12 Security Act of 2002 (6 U.S.C. 659) to identify and  
13 notify the entity at risk pursuant to the procedures  
14 within that section.

15 (3) REQUIRED INFORMATION.—A notification  
16 made under paragraph (1) shall include information  
17 on the identified security vulnerability and mitiga-  
18 tion techniques.

19 (d) PRIORITIZATION OF NOTIFICATIONS.—To the ex-  
20 tent practicable, the Director shall prioritize covered enti-  
21 ties for identification and notification activities under the  
22 pilot program established under this section.

23 (e) LIMITATION ON PROCEDURES.—No procedure,  
24 notification, or other authorities utilized in the execution  
25 of the pilot program established under subsection (a) shall

1 require an owner or operator of a vulnerable information  
2 system to take any action as a result of a notice of a secu-  
3 rity vulnerability made pursuant to subsection (c).

4 (f) **RULE OF CONSTRUCTION.**—Nothing in this sec-  
5 tion shall be construed to provide additional authorities  
6 to the Director to identify vulnerabilities or vulnerable sys-  
7 tems.

8 (g) **TERMINATION.**—The pilot program established  
9 under subsection (a) shall terminate on the date that is  
10 4 years after the date of enactment of this Act.

11 **SEC. 6106. RANSOMWARE THREAT MITIGATION ACTIVITIES.**

12 (a) **JOINT RANSOMWARE TASK FORCE.**—

13 (1) **IN GENERAL.**—Not later than 180 days  
14 after the date of enactment of this Act, the National  
15 Cyber Director, in consultation with the Attorney  
16 General and the Director of the Federal Bureau of  
17 Investigation, shall establish and chair the Joint  
18 Ransomware Task Force to coordinate an ongoing  
19 nationwide campaign against ransomware attacks,  
20 and identify and pursue opportunities for inter-  
21 national cooperation.

22 (2) **COMPOSITION.**—The Joint Ransomware  
23 Task Force shall consist of participants from Fed-  
24 eral agencies, as determined appropriate by the Na-

1 tional Cyber Director in consultation with the Sec-  
2 retary of Homeland Security.

3 (3) RESPONSIBILITIES.—The Joint  
4 Ransomware Task Force, utilizing only existing au-  
5 thorities of each participating agency, shall coordi-  
6 nate across the Federal Government the following  
7 activities:

8 (A) Prioritization of intelligence-driven op-  
9 erations to disrupt specific ransomware actors.

10 (B) Consult with relevant private sector,  
11 State, local, Tribal, and territorial governments  
12 and international stakeholders to identify needs  
13 and establish mechanisms for providing input  
14 into the Task Force.

15 (C) Identifying, in consultation with rel-  
16 evant entities, a list of highest threat  
17 ransomware entities updated on an ongoing  
18 basis, in order to facilitate—

19 (i) prioritization for Federal action by  
20 appropriate Federal agencies; and

21 (ii) identify metrics for success of said  
22 actions.

23 (D) Disrupting ransomware criminal ac-  
24 tors, associated infrastructure, and their fi-  
25 nances.

1 (E) Facilitating coordination and collabo-  
2 ration between Federal entities and relevant en-  
3 tities, including the private sector, to improve  
4 Federal actions against ransomware threats.

5 (F) Collection, sharing, and analysis of  
6 ransomware trends to inform Federal actions.

7 (G) Creation of after-action reports and  
8 other lessons learned from Federal actions that  
9 identify successes and failures to improve sub-  
10 sequent actions.

11 (H) Any other activities determined appro-  
12 priate by the task force to mitigate the threat  
13 of ransomware attacks against Federal and  
14 non-Federal entities.

15 (b) CLARIFYING PRIVATE SECTOR LAWFUL DEFEN-  
16 SIVE MEASURES.—Not later than 180 days after the date  
17 of enactment of this Act, the National Cyber Director, in  
18 coordination with the Secretary of Homeland Security and  
19 the Attorney General, shall submit to the Committee on  
20 Homeland Security and Governmental Affairs and the  
21 Committee on the Judiciary of the Senate and the Com-  
22 mittee on Homeland Security, the Committee on the Judi-  
23 ciary, and the Committee on Oversight and Reform of the  
24 House of Representatives a report that describes defensive  
25 measures that private sector actors can take when coun-

1 tering ransomware attacks and what laws need to be clari-  
2 fied to enable that action.

3 (c) **RULE OF CONSTRUCTION.**—Nothing in this sec-  
4 tion shall be construed to provide any additional authority  
5 to any Federal agency.

6 **SEC. 6107. CONGRESSIONAL REPORTING.**

7 (a) **REPORT ON STAKEHOLDER ENGAGEMENT.**—Not  
8 later than 30 days after the date on which the Director  
9 issues the final rule under section 2232(b) of the Home-  
10 land Security Act of 2002, as added by section 6103(b)  
11 of this title, the Director shall submit to the Committee  
12 on Homeland Security and Governmental Affairs of the  
13 Senate and the Committee on Homeland Security of the  
14 House of Representatives a report that describes how the  
15 Director engaged stakeholders in the development of the  
16 final rule.

17 (b) **REPORT ON OPPORTUNITIES TO STRENGTHEN**  
18 **SECURITY RESEARCH.**—Not later than 1 year after the  
19 date of enactment of this Act, the Director shall submit  
20 to the Committee on Homeland Security and Govern-  
21 mental Affairs of the Senate and the Committee on Home-  
22 land Security of the House of Representatives a report de-  
23 scribing how the National Cybersecurity and Communica-  
24 tions Integration Center established under section 2209  
25 of the Homeland Security Act of 2002 (6 U.S.C. 659) has

1 carried out activities under section 2231(a)(9) of the  
2 Homeland Security Act of 2002, as added by section  
3 6103(a) of this title, by proactively identifying opportuni-  
4 ties to use cyber incident data to inform and enable cyber-  
5 security research within the academic and private sector.

6 (c) REPORT ON RANSOMWARE VULNERABILITY  
7 WARNING PILOT PROGRAM.—Not later than 1 year after  
8 the date of enactment of this Act, and annually thereafter  
9 for the duration of the pilot program established under  
10 section 6105, the Director shall submit to the Committee  
11 on Homeland Security and Governmental Affairs of the  
12 Senate and the Committee on Homeland Security of the  
13 House of Representatives a report, which may include a  
14 classified annex, on the effectiveness of the pilot program,  
15 which shall include a discussion of the following:

16 (1) The effectiveness of the notifications under  
17 section 6105(c) in mitigating security vulnerabilities  
18 and the threat of ransomware.

19 (2) Identification of the most common  
20 vulnerabilities utilized in ransomware.

21 (3) The number of notifications issued during  
22 the preceding year.

23 (4) To the extent practicable, the number of  
24 vulnerable devices or systems mitigated under this  
25 pilot by the Agency during the preceding year.

1 (d) REPORT ON HARMONIZATION OF REPORTING  
2 REGULATIONS.—

3 (1) IN GENERAL.—Not later than 180 days  
4 after the date on which the National Cyber Director  
5 convenes the Council described in section  
6 1752(e)(1)(H) of the William M. (Mac) Thornberry  
7 National Defense Authorization Act for Fiscal Year  
8 2021 (6 U.S.C. 1500(e)(1)(H)), the National Cyber  
9 Director shall submit to the appropriate congress-  
10 sional committees a report that includes—

11 (A) a list of duplicative Federal cyber inci-  
12 dent reporting requirements on covered entities  
13 and entities that make a ransom payment;

14 (B) a description of any challenges in har-  
15 monizing the duplicative reporting require-  
16 ments;

17 (C) any actions the National Cyber Direc-  
18 tor intends to take to facilitate harmonizing the  
19 duplicative reporting requirements; and

20 (D) any proposed legislative changes nec-  
21 essary to address the duplicative reporting.

22 (2) RULE OF CONSTRUCTION.—Nothing in  
23 paragraph (1) shall be construed to provide any ad-  
24 ditional regulatory authority to any Federal agency.

25 (e) GAO REPORTS.—

1           (1) IMPLEMENTATION OF THIS ACT.—Not later  
2 than 2 years after the date of enactment of this Act,  
3 the Comptroller General of the United States shall  
4 submit to the Committee on Homeland Security and  
5 Governmental Affairs of the Senate and the Com-  
6 mittee on Homeland Security of the House of Rep-  
7 resentatives a report on the implementation of this  
8 Act and the amendments made by this Act.

9           (2) EXEMPTIONS TO REPORTING.—Not later  
10 than 1 year after the date on which the Director  
11 issues the final rule required under section 2232(b)  
12 of the Homeland Security Act of 2002, as added by  
13 section 6103 of this title, the Comptroller General of  
14 the United States shall submit to the Committee on  
15 Homeland Security and Governmental Affairs of the  
16 Senate and the Committee on Homeland Security of  
17 the House of Representatives a report on the exemp-  
18 tions to reporting under paragraphs (2) and (5) of  
19 section 2232(a) of the Homeland Security Act of  
20 2002, as added by section 6103 of this title, which  
21 shall include—

22                   (A) to the extent practicable, an evaluation  
23 of the quantity of incidents not reported to the  
24 Federal Government;

1 (B) an evaluation of the impact on im-  
2 pacted entities, homeland security, and the na-  
3 tional economy of the ransomware criminal eco-  
4 system of incidents and ransom payments, in-  
5 cluding a discussion on the scope of impact of  
6 incidents that were not reported to the Federal  
7 Government;

8 (C) an evaluation of the burden, financial  
9 and otherwise, on entities required to report  
10 cyber incidents under this Act, including an  
11 analysis of entities that meet the definition of  
12 a small organization and would be exempt from  
13 ransom payment reporting but not for being a  
14 covered entity; and

15 (D) a description of the consequences and  
16 effects of the exemptions.

17 (f) REPORT ON EFFECTIVENESS OF ENFORCEMENT  
18 MECHANISMS.—Not later than 1 year after the date on  
19 which the Director issues the final rule required under sec-  
20 tion 2232(b) of the Homeland Security Act of 2002, as  
21 added by section 6103 of this title, the Director shall sub-  
22 mit to the Committee on Homeland Security and Govern-  
23 mental Affairs of the Senate and the Committee on Home-  
24 land Security of the House of Representatives a report on  
25 the effectiveness of the enforcement mechanisms within

1 section 2234 of the Homeland Security Act of 2002, as  
2 added by section 6103 of this title.

3 **TITLE LXII—CISA TECHNICAL**  
4 **CORRECTIONS AND IMPROVE-**  
5 **MENTS ACT OF 2021**

6 **SEC. 6201. SHORT TITLE.**

7 This title may be cited as the “CISA Technical Cor-  
8 rections and Improvements Act of 2021”.

9 **SEC. 6202. REDESIGNATIONS.**

10 (a) IN GENERAL.—Subtitle A of title XXII of the  
11 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)  
12 is amended—

13 (1) by redesignating section 2217 (6 U.S.C.  
14 665f) as section 2220;

15 (2) by redesignating section 2216 (6 U.S.C.  
16 665e) as section 2219;

17 (3) by redesignating the fourth section 2215  
18 (relating to Sector Risk Management Agencies) (6  
19 U.S.C. 665d) as section 2218;

20 (4) by redesignating the third section 2215 (re-  
21 lating to the Cybersecurity State Coordinator) (6  
22 U.S.C. 665c) as section 2217; and

23 (5) by redesignating the second section 2215  
24 (relating to the Joint Cyber Planning Office) (6  
25 U.S.C. 665b) as section 2216.

1 (b) TECHNICAL AND CONFORMING AMENDMENTS.—  
2 Section 2202(c) of the Homeland Security Act of 2002  
3 (6 U.S.C. 652(c)) is amended—

4 (1) in the first paragraph (12), by striking  
5 “section 2215” and inserting “section 2217”; and

6 (2) by redesignating the second and third para-  
7 graphs (12) as paragraphs (13) and (14), respec-  
8 tively.

9 (c) ADDITIONAL TECHNICAL AMENDMENT.—

10 (1) AMENDMENT.—Section 904(b)(1) of the  
11 DOTGOV Act of 2020 (title IX of division U of  
12 Public Law 116–260) is amended, in the matter pre-  
13 ceding subparagraph (A), by striking “Homeland  
14 Security Act” and inserting “Homeland Security Act  
15 of 2002”.

16 (2) EFFECTIVE DATE.—The amendment made  
17 by paragraph (1) shall take effect as if enacted as  
18 part of the DOTGOV Act of 2020 (title IX of divi-  
19 sion U of Public Law 116–260).

20 **SEC. 6203. CONSOLIDATION OF DEFINITIONS.**

21 (a) IN GENERAL.—Title XXII of the Homeland Se-  
22 curity Act of 2002 (6 U.S.C. 651) is amended by inserting  
23 before the subtitle A heading the following:

1 **“SEC. 2200. DEFINITIONS.**

2 “Except as otherwise specifically provided, in this  
3 title:

4 “(1) AGENCY.—The term ‘Agency’ means the  
5 Cybersecurity and Infrastructure Security Agency.

6 “(2) AGENCY INFORMATION.—The term ‘agen-  
7 cy information’ means information collected or main-  
8 tained by or on behalf of an agency.

9 “(3) AGENCY INFORMATION SYSTEM.—The  
10 term ‘agency information system’ means an informa-  
11 tion system used or operated by an agency or by an-  
12 other entity on behalf of an agency.

13 “(4) APPROPRIATE CONGRESSIONAL COMMIT-  
14 TEES.—The term ‘appropriate congressional com-  
15 mittees’ means—

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

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

20 “(5) CLOUD SERVICE PROVIDER.—The term  
21 ‘cloud service provider’ means an entity offering  
22 products or services related to cloud computing, as  
23 defined by the National Institutes of Standards and  
24 Technology in NIST Special Publication 800–145  
25 and any amendatory or superseding document relat-  
26 ing thereto.

1           “(6) CRITICAL INFRASTRUCTURE INFORMA-  
2           TION.—The term ‘critical infrastructure information’  
3           means information not customarily in the public do-  
4           main and related to the security of critical infra-  
5           structure or protected systems, including—

6                   “(A) actual, potential, or threatened inter-  
7                   ference with, attack on, compromise of, or inca-  
8                   pacitation of critical infrastructure or protected  
9                   systems by either physical or computer-based  
10                  attack or other similar conduct (including the  
11                  misuse of or unauthorized access to all types of  
12                  communications and data transmission systems)  
13                  that violates Federal, State, or local law, harms  
14                  interstate commerce of the United States, or  
15                  threatens public health or safety;

16                  “(B) the ability of any critical infrastruc-  
17                  ture or protected system to resist such inter-  
18                  ference, compromise, or incapacitation, includ-  
19                  ing any planned or past assessment, projection,  
20                  or estimate of the vulnerability of critical infra-  
21                  structure or a protected system, including secu-  
22                  rity testing, risk evaluation thereto, risk man-  
23                  agement planning, or risk audit; or

24                  “(C) any planned or past operational prob-  
25                  lem or solution regarding critical infrastructure

1 or protected systems, including repair, recovery,  
2 reconstruction, insurance, or continuity, to the  
3 extent it is related to such interference, com-  
4 promise, or incapacitation.

5 “(7) CYBER THREAT INDICATOR.—The term  
6 ‘cyber threat indicator’ means information that is  
7 necessary to describe or identify—

8 “(A) malicious reconnaissance, including  
9 anomalous patterns of communications that ap-  
10 pear to be transmitted for the purpose of gath-  
11 ering technical information related to a cyberse-  
12 curity threat or security vulnerability;

13 “(B) a method of defeating a security con-  
14 trol or exploitation of a security vulnerability;

15 “(C) a security vulnerability, including  
16 anomalous activity that appears to indicate the  
17 existence of a security vulnerability;

18 “(D) a method of causing a user with le-  
19 gitimate access to an information system or in-  
20 formation that is stored on, processed by, or  
21 transiting an information system to unwittingly  
22 enable the defeat of a security control or exploi-  
23 tation of a security vulnerability;

24 “(E) malicious cyber command and con-  
25 trol;

1           “(F) the actual or potential harm caused  
2           by an incident, including a description of the in-  
3           formation exfiltrated as a result of a particular  
4           cybersecurity threat;

5           “(G) any other attribute of a cybersecurity  
6           threat, if disclosure of such attribute is not oth-  
7           erwise prohibited by law; or

8           “(H) any combination thereof.

9           “(8) CYBERSECURITY PURPOSE.—The term ‘cy-  
10          bersecurity purpose’ means the purpose of protecting  
11          an information system or information that is stored  
12          on, processed by, or transiting an information sys-  
13          tem from a cybersecurity threat or security vulner-  
14          ability.

15          “(9) CYBERSECURITY RISK.—The term ‘cyber-  
16          security risk’—

17                 “(A) means threats to and vulnerabilities  
18                 of information or information systems and any  
19                 related consequences caused by or resulting  
20                 from unauthorized access, use, disclosure, deg-  
21                 radation, disruption, modification, or destruc-  
22                 tion of such information or information sys-  
23                 tems, including such related consequences  
24                 caused by an act of terrorism; and

1           “(B) does not include any action that sole-  
2 ly involves a violation of a consumer term of  
3 service or a consumer licensing agreement.

4           “(10) CYBERSECURITY THREAT.—

5           “(A) IN GENERAL.—Except as provided in  
6 subparagraph (B), the term ‘cybersecurity  
7 threat’ means an action, not protected by the  
8 First Amendment to the Constitution of the  
9 United States, on or through an information  
10 system that may result in an unauthorized ef-  
11 fort to adversely impact the security, avail-  
12 ability, confidentiality, or integrity of an infor-  
13 mation system or information that is stored on,  
14 processed by, or transiting an information sys-  
15 tem.

16           “(B) EXCLUSION.—The term ‘cybersecu-  
17 rity threat’ does not include any action that  
18 solely involves a violation of a consumer term of  
19 service or a consumer licensing agreement.

20           “(11) DEFENSIVE MEASURE.—

21           “(A) IN GENERAL.—Except as provided in  
22 subparagraph (B), the term ‘defensive measure’  
23 means an action, device, procedure, signature,  
24 technique, or other measure applied to an infor-  
25 mation system or information that is stored on,

1 processed by, or transiting an information sys-  
2 tem that detects, prevents, or mitigates a  
3 known or suspected cybersecurity threat or se-  
4 curity vulnerability.

5 “(B) EXCLUSION.—The term ‘defensive  
6 measure’ does not include a measure that de-  
7 stroys, renders unusable, provides unauthorized  
8 access to, or substantially harms an information  
9 system or information stored on, processed by,  
10 or transiting such information system not  
11 owned by—

12 “(i) the entity operating the measure;  
13 or

14 “(ii) another entity or Federal entity  
15 that is authorized to provide consent and  
16 has provided consent to that private entity  
17 for operation of such measure.

18 “(12) HOMELAND SECURITY ENTERPRISE.—  
19 The term ‘Homeland Security Enterprise’ means rel-  
20 evant governmental and nongovernmental entities in-  
21 volved in homeland security, including Federal,  
22 State, local, and Tribal government officials, private  
23 sector representatives, academics, and other policy  
24 experts.

1           “(13) INCIDENT.—The term ‘incident’ means  
2           an occurrence that actually or imminently jeopard-  
3           izes, without lawful authority, the integrity, con-  
4           fidentiality, or availability of information on an in-  
5           formation system, or actually or imminently jeopard-  
6           izes, without lawful authority, an information sys-  
7           tem.

8           “(14) INFORMATION SHARING AND ANALYSIS  
9           ORGANIZATION.—The term ‘Information Sharing  
10          and Analysis Organization’ means any formal or in-  
11          formal entity or collaboration created or employed by  
12          public or private sector organizations, for purposes  
13          of—

14                 “(A) gathering and analyzing critical infra-  
15                 structure information, including information re-  
16                 lated to cybersecurity risks and incidents, in  
17                 order to better understand security problems  
18                 and interdependencies related to critical infra-  
19                 structure, including cybersecurity risks and in-  
20                 cidents, and protected systems, so as to ensure  
21                 the availability, integrity, and reliability thereof;

22                 “(B) communicating or disclosing critical  
23                 infrastructure information, including cybersecu-  
24                 rity risks and incidents, to help prevent, detect,  
25                 mitigate, or recover from the effects of a inter-

1           ference, compromise, or a incapacitation prob-  
2           lem related to critical infrastructure, including  
3           cybersecurity risks and incidents, or protected  
4           systems; and

5                   “(C) voluntarily disseminating critical in-  
6           frastructure information, including cybersecu-  
7           rity risks and incidents, to its members, State,  
8           local, and Federal Governments, or any other  
9           entities that may be of assistance in carrying  
10          out the purposes specified in subparagraphs (A)  
11          and (B).

12                   “(15) INFORMATION SYSTEM.—The term ‘infor-  
13          mation system’ has the meaning given the term in  
14          section 3502 of title 44, United States Code.

15                   “(16) INTELLIGENCE COMMUNITY.—The term  
16          ‘intelligence community’ has the meaning given the  
17          term in section 3(4) of the National Security Act of  
18          1947 (50 U.S.C. 3003(4)).

19                   “(17) MANAGED SERVICE PROVIDER.—The  
20          term ‘managed service provider’ means an entity  
21          that delivers services, such as network, application,  
22          infrastructure, or security services, via ongoing and  
23          regular support and active administration on the  
24          premises of a customer, in the data center of the en-

1       tity (such as hosting), or in a third party data cen-  
2       ter.

3               “(18) MONITOR.—The term ‘monitor’ means to  
4       acquire, identify, or scan, or to possess, information  
5       that is stored on, processed by, or transiting an in-  
6       formation system.

7               “(19) NATIONAL CYBERSECURITY ASSET RE-  
8       SPONSE ACTIVITIES.—The term ‘national cybersecu-  
9       rity asset response activities’ means—

10               “(A) furnishing cybersecurity technical as-  
11       sistance to entities affected by cybersecurity  
12       risks to protect assets, mitigate vulnerabilities,  
13       and reduce impacts of cyber incidents;

14               “(B) identifying other entities that may be  
15       at risk of an incident and assessing risk to the  
16       same or similar vulnerabilities;

17               “(C) assessing potential cybersecurity risks  
18       to a sector or region, including potential cas-  
19       cading effects, and developing courses of action  
20       to mitigate such risks;

21               “(D) facilitating information sharing and  
22       operational coordination with threat response;  
23       and

24               “(E) providing guidance on how best to  
25       utilize Federal resources and capabilities in a

1           timely, effective manner to speed recovery from  
2           cybersecurity risks.

3           “(20) NATIONAL SECURITY SYSTEM.—The term  
4           ‘national security system’ has the meaning given the  
5           term in section 11103 of title 40, United States  
6           Code.

7           “(21) RANSOM PAYMENT.—The term ‘ransom  
8           payment’ means the transmission of any money or  
9           other property or asset, including virtual currency,  
10          or any portion thereof, which has at any time been  
11          delivered as ransom in connection with a  
12          ransomware attack.

13          “(22) RANSOMWARE ATTACK.—The term  
14          ‘ransomware attack’—

15                 “(A) means a cyber incident that includes  
16                 the threat of use of unauthorized or malicious  
17                 code on an information system, or the threat of  
18                 use of another digital mechanism such as a de-  
19                 nial of service attack, to interrupt or disrupt  
20                 the operations of an information system or com-  
21                 promise the confidentiality, availability, or in-  
22                 tegrity of electronic data stored on, processed  
23                 by, or transiting an information system to ex-  
24                 tort a demand for a ransom payment; and

1           “(B) does not include any such event  
2           where the demand for payment is made by a  
3           Federal Government entity, good faith security  
4           research, or in response to an invitation by the  
5           owner or operator of the information system for  
6           third parties to identify vulnerabilities in the in-  
7           formation system.

8           “(23) SECTOR RISK MANAGEMENT AGENCY.—  
9           The term ‘Sector Risk Management Agency’ means  
10          a Federal department or agency, designated by law  
11          or Presidential directive, with responsibility for pro-  
12          viding institutional knowledge and specialized exper-  
13          tise of a sector, as well as leading, facilitating, or  
14          supporting programs and associated activities of its  
15          designated critical infrastructure sector in the all  
16          hazards environment in coordination with the De-  
17          partment.

18          “(24) SECURITY VULNERABILITY.—The term  
19          ‘security vulnerability’ means any attribute of hard-  
20          ware, software, process, or procedure that could en-  
21          able or facilitate the defeat of a security control.

22          “(25) SHARING.—The term ‘sharing’ (including  
23          all conjugations thereof) means providing, receiving,  
24          and disseminating (including all conjugations of each  
25          such terms).

1           “(26) SUPPLY CHAIN COMPROMISE.—The term  
2           ‘supply chain compromise’ means a cyber incident  
3           within the supply chain of an information technology  
4           system whereby an adversary jeopardizes the con-  
5           fidentiality, integrity, or availability of the informa-  
6           tion technology system or the information the sys-  
7           tem processes, stores, or transmits, and can occur at  
8           any point during the life cycle.

9           “(27) VIRTUAL CURRENCY.—The term ‘virtual  
10          currency’ means the digital representation of value  
11          that functions as a medium of exchange, a unit of  
12          account, or a store of value.

13          “(28) VIRTUAL CURRENCY ADDRESS.—The  
14          term ‘virtual currency address’ means a unique pub-  
15          lic cryptographic key identifying the location to  
16          which a virtual currency payment can be made.”.

17          (b) TECHNICAL AND CONFORMING AMENDMENTS.—  
18          The Homeland Security Act of 2002 (6 U.S.C. 101 et  
19          seq.) is amended—

20                 (1) by amending section 2201 to read as fol-  
21          lows:

22          **“SEC. 2201. DEFINITION.**

23                 “In this subtitle, the term ‘Cybersecurity Advisory  
24          Committee’ means the advisory committee established  
25          under section 2219(a).”;

1 (2) in section 2202—

2 (A) in subsection (a)(1), by striking “(in  
3 this subtitle referred to as the Agency)”;

4 (B) in subsection (f)—

5 (i) in paragraph (1), by inserting  
6 “Executive” before “Assistant Director”;

7 and

8 (ii) in paragraph (2), by inserting  
9 “Executive” before “Assistant Director”;

10 (3) in section 2203(a)(2), by striking “as the  
11 ‘Assistant Director’” and inserting “as the ‘Execu-  
12 tive Assistant Director’”;

13 (4) in section 2204(a)(2), by striking “as the  
14 ‘Assistant Director’” and inserting “as the ‘Execu-  
15 tive Assistant Director’”;

16 (5) in section 2209—

17 (A) by striking subsection (a);

18 (B) by redesignating subsections (b)  
19 through (o) as subsections (a) through (n), re-  
20 spectively;

21 (C) in subsection (c)(1)(A)(iii), as so re-  
22 designated, by striking “, as that term is de-  
23 fined under section 3(4) of the National Secu-  
24 rity Act of 1947 (50 U.S.C. 3003(4))”;

1 (D) in subsection (d), as so redesignated,  
2 in the matter preceding paragraph (1), by strik-  
3 ing “subsection (c)” and inserting “subsection  
4 (b)”;

5 (E) in subsection (j), as so redesignated,  
6 by striking “subsection (c)(8)” and inserting  
7 “subsection (b)(8)”;

8 (F) in subsection (n), as so redesignated—

9 (i) in paragraph (2)(A), by striking  
10 “subsection (c)(12)” and inserting “sub-  
11 section (b)(12)”;

12 (ii) in paragraph (3)(B)(i), by striking  
13 “subsection (c)(12)” and inserting “sub-  
14 section (b)(12)”;

15 (6) in section 2210—

16 (A) by striking subsection (a);

17 (B) by redesignating subsections (b)  
18 through (d) as subsections (a) through (c), re-  
19 spectively;

20 (C) in subsection (b), as so redesignated—

21 (i) by striking “information sharing  
22 and analysis organizations (as defined in  
23 section 2222(5))” and inserting “Informa-  
24 tion Sharing and Analysis Organizations”;  
25 and

1 (ii) by striking “(as defined in section  
2 2209)”; and

3 (D) in subsection (c), as so redesignated,  
4 by striking “subsection (c)” and inserting “sub-  
5 section (b)”;

6 (7) in section 2211, by striking subsection (h);

7 (8) in section 2212, by striking “information  
8 sharing and analysis organizations (as defined in  
9 section 2222(5))” and inserting “Information Shar-  
10 ing and Analysis Organizations”;

11 (9) in section 2213—

12 (A) by striking subsection (a);

13 (B) by redesignating subsections (b)  
14 through (f) as subsections (a) through (e); re-  
15 spectively;

16 (C) in subsection (b), as so redesignated,  
17 by striking “subsection (b)” each place it ap-  
18 pears and inserting “subsection (a)”;

19 (D) in subsection (c), as so redesignated,  
20 in the matter preceding paragraph (1), by strik-  
21 ing “subsection (b)” and inserting “subsection  
22 (a)”;

23 (E) in subsection (d), as so redesignated—

24 (i) in paragraph (1)—

1 (I) in the matter preceding sub-  
2 paragraph (A), by striking “sub-  
3 section (c)(2)” and inserting “sub-  
4 section (b)(2)”;

5 (II) in subparagraph (A), by  
6 striking “subsection (c)(1)” and in-  
7 serting “subsection (b)(1)”;

8 (III) in subparagraph (B), by  
9 striking “subsection (c)(2)” and in-  
10 serting “subsection (b)(2)”;

11 (ii) in paragraph (2), by striking  
12 “subsection (c)(2)” and inserting “sub-  
13 section (b)(2)”;

14 (10) in section 2216, as so redesignated—

15 (A) by striking subsection (a);

16 (B) by redesignating subsections (b)  
17 through (h) as subsections (a) through (g), re-  
18 spectively;

19 (C) in subsection (a), as so redesignated—

20 (i) in the matter preceding paragraph  
21 (1), by striking “subsection (e)” and in-  
22 serting “subsection (d)”;

23 (ii) in paragraph (1), by striking  
24 “subsection (c)” and inserting “subsection  
25 (b)”;

1 (iii) in paragraph (2), by striking  
2 “subsection (c)” and inserting “subsection  
3 (b)”;

4 (D) in subsection (b)(4), as so redesignated—  
5 nated—

6 (i) by striking “subsection (e)” and  
7 inserting “subsection (d)”;

8 (ii) by striking “subsection (h)” and  
9 inserting “subsection (g)”;

10 (E) in subsection (d), as so redesignated,  
11 by striking “subsection (b)(1)” each place it ap-  
12 pears and inserting “subsection (a)(1)”;

13 (F) in subsection (e), as so redesignated—

14 (i) by striking “subsection (b)” and  
15 inserting “subsection (a)”;

16 (ii) by striking “subsection (e)” and  
17 inserting “subsection (d)”;

18 (iii) by striking “subsection (b)(1)”  
19 and inserting “subsection (a)(1)”;

20 (G) in subsection (f), as so redesignated,  
21 by striking “subsection (c)” and inserting “sub-  
22 section (b)”;

23 (11) in section 2217, as so redesignated, by  
24 striking subsection (f) and inserting the following:

1       “(f) CYBER DEFENSE OPERATION DEFINED.—In  
2 this section, the term ‘cyber defense operation’ means the  
3 use of a defensive measure.”; and

4           (12) in section 2222—

5           (A) by striking paragraphs (3), (5), and  
6           (8);

7           (B) by redesignating paragraph (4) as  
8           paragraph (3); and

9           (C) by redesignating paragraphs (6) and  
10          (7) as paragraphs (4) and (5), respectively.

11       (c) TABLE OF CONTENTS AMENDMENTS.—The table  
12 of contents in section 1(b) of the Homeland Security Act  
13 of 2002 (Public Law 107–296; 116 Stat. 2135) is amend-  
14 ed—

15           (1) by inserting before the item relating to sub-  
16          title A of title XXII the following:

“Sec. 2200. Definitions.”;

17           (2) by striking the item relating to section 2201  
18          and inserting the following:

“Sec. 2201. Definition.”; and

19           (3) by striking the second item relating to sec-  
20          tion 2215 and all that follows through the item re-  
21          lating to section 2217 and inserting the following:

“Sec. 2216. Cybersecurity State Coordinator.

“Sec. 2217. Joint Cyber Planning Office.

“Sec. 2218. Duties and authorities relating to .gov internet domain.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.”.

1 (d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—  
2 Section 102 of the Cybersecurity Act of 2015 (6 U.S.C.  
3 1501) is amended—

4 (1) by striking paragraphs (4) through (7) and  
5 inserting the following:

6 “(4) CYBERSECURITY PURPOSE.—The term ‘cy-  
7 bersecurity purpose’ has the meaning given the term  
8 in section 2200 of the Homeland Security Act of  
9 2002.

10 “(5) CYBERSECURITY THREAT.—The term ‘cy-  
11 bersecurity threat’ has the meaning given the term  
12 in section 2200 of the Homeland Security Act of  
13 2002.

14 “(6) CYBER THREAT INDICATOR.—The term  
15 ‘cyber threat indicator’ has the meaning given the  
16 term in section 2200 of the Homeland Security Act  
17 of 2002.

18 “(7) DEFENSIVE MEASURE.—The term ‘defen-  
19 sive measure’ has the meaning given the term in sec-  
20 tion 2200 of the Homeland Security Act of 2002.”;

21 (2) by striking paragraph (13) and inserting  
22 the following:

23 “(13) MONITOR.— The term ‘monitor’ has the  
24 meaning given the term in section 2200 of the  
25 Homeland Security Act of 2002.”; and



1 (ii) in paragraph (4), by striking “sec-  
2 tion 2210(b)(1)” and inserting “section  
3 2210(a)(1)”; and

4 (iii) in paragraph (5), by striking  
5 “section 2213(b)” and inserting “section  
6 2213(a)”; and

7 (B) in subsection (c)(1)(A)(vi), by striking  
8 “section 2213(c)(5)” and inserting “section  
9 2213(b)(5)”; and

10 (4) in section 227(b) (6 U.S.C. 1525(b)), by  
11 striking “section 2213(d)(2)” and inserting “section  
12 2213(e)(2)”.

13 (b) PUBLIC HEALTH SERVICE ACT.—Section  
14 2811(b)(4)(D) of the Public Health Service Act (42  
15 U.S.C. 300hh–10(b)(4)(D)) is amended by striking “sec-  
16 tion 228(c) of the Homeland Security Act of 2002 (6  
17 U.S.C. 149(c))” and inserting “section 2210(c) of the  
18 Homeland Security Act of 2002”.

19 (c) WILLIAM M. (MAC) THORNBERRY NATIONAL DE-  
20 FENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—  
21 Section 9002 of the William M. (Mac) Thornberry Na-  
22 tional Defense Authorization Act for Fiscal Year 2021 (6  
23 U.S.C. 652a) is amended—

24 (1) in subsection (a)—

1 (A) in paragraph (5), by striking “section  
2 2222(5) of the Homeland Security Act of 2002  
3 (6 U.S.C. 671(5))” and inserting “section 2200  
4 of the Homeland Security Act of 2002”; and

5 (B) by amending paragraph (7) to read as  
6 follows:

7 “(7) SECTOR RISK MANAGEMENT AGENCY.—  
8 The term ‘Sector Risk Management Agency’ has the  
9 meaning given the term in section 2200 of the  
10 Homeland Security Act of 2002.”;

11 (2) in subsection (e)(3)(B), by striking “section  
12 2201(5) of the Homeland Security Act of 2002 (6  
13 U.S.C. 651(5))” and inserting “section 2200 of the  
14 Homeland Security Act of 2002”; and

15 (3) in subsection (d)—

16 (A) by striking “section 2215” and insert-  
17 ing “section 2218”; and

18 (B) by striking “, as added by this sec-  
19 tion”.

20 (d) NATIONAL SECURITY ACT OF 1947.—Section  
21 113B of the National Security Act of 1947 (50 U.S.C.  
22 3049a(b)(4)) is amended by striking “section 226 of the  
23 Homeland Security Act of 2002 (6 U.S.C. 147)” and in-  
24 serting “section 2206 of the Homeland Security Act of  
25 2002”.

1           (e) IOT CYBERSECURITY IMPROVEMENT ACT OF  
2 2020.—Section 5(b)(3) of the IoT Cybersecurity Improve-  
3 ment Act of 2020 (15 U.S.C. 278g–3e) is amended by  
4 striking “section 2209(m)” and inserting “section  
5 2209(l)”.

6           (f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of  
7 the Small Business Act (15 U.S.C. 648(a)(8)(B)) is  
8 amended by striking “section 2209(a)” and inserting “sec-  
9 tion 2200”.

10          (g) TITLE 46.—Section 70101(2) of title 46, United  
11 States Code, is amended by striking “section 227 of the  
12 Homeland Security Act of 2002 (6 U.S.C. 148)” and in-  
13 serting “section 2200 of the Homeland Security Act of  
14 2002”.