Calendar No. 673

117TH CONGRESS
2D SESSION

S. 2902

[Report No. 117–274]

To modernize Federal information security management, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 29, 2021

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

DECEMBER 19, 2022

Reported by Mr. PETERS, with an amendment

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

A BILL

To modernize Federal information security management, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~**SECTION 1. SHORT TITLE.**~~

~~This Act may be cited as the "Federal Information Security Modernization Act of 2021".~~

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act, unless otherwise specified:

(1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term ''additional cybersecurity procedure'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this Act.

(2) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

(B) the Committee on Oversight and Reform of the House of Representatives; and

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

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

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

(6) PENETRATION TEST.—The term ''penetration test'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this Act.

(7) THREAT HUNTING.—The term ''threat hunting'' means proactively and iteratively searching

for threats to systems that evade detection by automated threat detection systems.

(8) VERIFICATION SPECIFICATION.—The term ''verification specification'' means a specification developed under section 11331(f) of title 40, United States Code, as amended by this Act.

TITLE I—UPDATES TO FISMA

SEC. 101. TITLE 44 AMENDMENTS.

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

(1) in section 3504—

(A) in subsection (a)(1)(B)(v), by striking ''confidentiality, security, disclosure, and sharing of information'' and inserting ''disclosure, sharing of information, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, confidentiality and security'';

(B) in subsection (b)(2)(B), by inserting ''in coordination with the Director of the Cybersecurity and Infrastructure Security Agency'' after ''standards for security'';

(C) in subsection (g), by striking paragraph (1) and inserting the following:

''(1) with respect to information collected or maintained by or for agencies—

''(A) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, disclosure, and sharing of the information; and

''(B) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, develop and oversee policies, principles, standards, and guidelines on confidentiality and security of the information; and''; and

(D) in subsection (h)(1)—

(i) in the matter preceding subparagraph (A)—

(I) by inserting ''the Director of the Cybersecurity and Infrastructure Security Agency,'' before ''the Director''; and

(II) by inserting a comma before ''and the Administrator''; and

(ii) in subparagraph (A), by inserting ''security and'' after ''information technology'';

(2) in section 3505—

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

(i) in subparagraph (B)—

(I) by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' after ''Comptroller General''; and

(II) by striking ''and'' at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning.''; and

(B) by striking the second subsection designated as subsection (c);

(3) in section 3506—

(A) in subsection (b)—

(i) in paragraph (1)(C), by inserting '', availability'' after ''integrity''; and

(ii) in paragraph (4), by inserting ''the Director of the Cybersecurity and In-

frastructure Security Agency,'' after ''General Services,''; and

(B) in subsection (h)(3), by inserting ''security,'' after ''efficiency,'';

(4) in section 3513—

(A) in subsection (a), by inserting ''the Director of the Cybersecurity and Infrastructure Security Agency,'' before ''the Administrator of General Services'';

(B) by redesignating subsection (c) as subsection (d); and

(C) by inserting after subsection (b) the following:

''(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.''; and

(5) in section 3520A(b)—

(A) in paragraph (1), by striking '', protection'';

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

(C) by inserting after paragraph (1) the following:

"(2) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, establish Governmentwide best practices for the protection of data;".

(b) SUCHAPTER H DEFINITIONS.—

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

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

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

"(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems, such as continuous threat hunting, increased network segmentation, endpoint detection and response, or persistent penetration testing.";

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

''(7) The term 'high value asset' means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

''(8) The term 'major incident' has the meaning given the term in guidance issued by the Director under section 3598(a).'';

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

''(10) The term 'penetration test' means a specialized type of assessment that—

''(A) is conducted on an information system or a component of an information system; and

''(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information system or a component of an information system that could be exploited.''; and

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

''(12) The term 'shared service' means a business or mission function that is provided for use by multiple organizations within or between agencies.

''(13) The term 'verification specification' means a specification developed under section 11331(f) of title 40.''.

(2) CONFORMING AMENDMENTS.—

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

(B) TITLE 10.—

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

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

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended

by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

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

(C) HIGH-PERFORMANCE COMPUTING ACT OF 1991.—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking ''section 3552(b)(6)(A)(i)'' and inserting ''section 3552(b)(9)(A)(i)''.

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

(E) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(F) IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

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

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''; and

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

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

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

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

(ii) in subsection (f)—

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

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

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

(1) in section 3551—

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

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

''(3) recognize the role of the Cybersecurity and Infrastructure Security Agency as the lead cybersecurity entity for operational coordination across the Federal Government;'';

(C) in paragraph (5), as so redesignated, by striking ''diagnose and improve'' and inserting ''integrate, deliver, diagnose, and improve'';

(D) in paragraph (6), as so redesignated, by striking ''and'' at the end; and

(E) by adding at the end the following:

''(8) recognize that each agency has specific mission requirements and, at times, unique cybersecurity requirements to meet the mission of the agency;

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

''(10) recognize that—

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

''(B) in accounting for the differences described in subparagraph (A) and ensuring overall Federal cybersecurity—

''(i) the Office of Management and Budget is the leader for policy development and oversight of Federal cybersecurity;

''(ii) the Cybersecurity and Infrastructure Security Agency is the leader for implementing operations at agencies; and

''(iii) the National Cyber Director is responsible for developing the overall cybersecurity strategy of the United States and advising the President on matters relating to cybersecurity.'';

(2) in section 3553, as amended by section 1705 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283)—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by striking ''developing and'' and inserting ''in coordination with the Director of the Cybersecurity and Infrastructure Security Agency,''; and

(II) by inserting ''and associated verification specifications'' before ''promulgated''; and

(ii) in paragraph (5), by inserting '', in coordination with the Director of the Cybersecurity and Infrastructure Security Agency,'' before ''agency compliance'';

(B) in subsection (b)—

(i) by striking the subsection heading and inserting ''CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'';

(ii) in the matter preceding paragraph (1), by striking ''the Secretary'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(iii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''and reporting requirements under subchapter IV of this title'' after ''section 3556''; and

(II) in subparagraph (D), by striking ''the Director or Secretary'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(iv) in paragraph (5), by striking ''coordinating'' and inserting ''leading the coordination of'';

(v) in paragraph (6)—

(I) in the matter preceding subparagraph (A), by inserting ''and

verifications specifications'' before ''promulgated under'';

(II) in subparagraph (C), by striking ''and'' at the end;

(III) in subparagraph (D), by adding ''and'' at the end; and

(IV) by adding at the end the following:

''(E) taking any other action that the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director—

''(i) may determine necessary; and

''(ii) is authorized to perform;'';

(vi) in paragraph (8), by striking ''the Secretary's discretion'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency's discretion''; and

(vii) in paragraph (9), by striking ''as the Director or the Secretary, in consultation with the Director,'' and inserting ''as the Director of the Cybersecurity and Infrastructure Security Agency'';

(C) in subsection (c)—

(i) in paragraph (4), by striking ''and'' at the end;

(ii) by redesignating paragraph (5) as paragraph (7); and

(iii) by inserting after paragraph (4) the following:

''(5) an assessment of agency use of automated verification of standards for the standards promulgated under section 11331 of title 40 using verification specifications;

''(6) a summary of each assessment of Federal risk posture performed under subsection (i); and'';

(D) in subsection (f)(2)(B), by striking ''conflict with'' and inserting ''reduce the security posture of agencies established under'';

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

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

''(i) FEDERAL RISK ASSESSMENTS.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall perform, on an ongoing and continuous basis, assessments of Federal risk pos-

ture using any available information on the cybersecurity posture of agencies, including—

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

"(2) any vulnerability information relating to the systems of an agency that is known by the agency;

"(3) analysis of incident information under section 3597;

"(4) evaluation of penetration testing performed under section 3559A;

"(5) evaluation of vulnerability disclosure program information under section 3559B;

"(6) evaluation of agency threat hunting results;

"(7) evaluation of Federal and non-Federal threat intelligence;

"(8) data on compliance with standards issued under section 11331 of title 40 that, when appropriate, uses verification specifications;

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

"(10) any other information the Secretary determines relevant."; and

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

(i) by striking ''regarding the specific'' and inserting ''that includes a summary of—

''(1) the specific'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and'' and

(iii) by adding at the end the following:

''(2) the trends identified in the Federal risk assessment performed under subsection (i).'';

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by redesignating subparagraphs (A), (B), and (C) as subparagraphs (B), (C), and (D), respectively;

(II) by inserting before subparagraph (B), as so redesignated, the following:

''(A) performing, not less frequently than once every 2 years or based on a significant change to system architecture or security posture, an agency system risk assessment that—

"(i) identifies and documents the high value assets of the agency using guidance from the Director;

"(ii) evaluates the data assets inventoried under section 3511 of title 44 for sensitivity to compromises in confidentiality, integrity, and availability;

"(iii) identifies agency systems that have access to or hold the data assets inventoried under section 3511 of title 44;

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

"(v) evaluates the vulnerability of agency systems and data, including high value assets, based on—

"(I) the results of penetration testing performed by the Department of Homeland Security under section 3553(b)(9);

"(II) the results of penetration testing performed under section 3559A;

''(III) information provided to the agency through the vulnerability disclosure program of the agency under section 3559B;

''(IV) incidents; and

''(V) any other vulnerability information relating to agency systems that is known to the agency;

''(vi) assesses the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (iv) and the agency systems identified under clause (iii); and

''(vii) assesses the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or operational reliance on the operations of the system or data in the system;'';

(III) in subparagraph (B), as so redesignated—

(aa) in the matter preceding clause (i), by striking ''providing

information'' and inserting ''using information from the assessment conducted under subparagraph (A), providing, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, information'';

(bb) in clause (i), by striking ''and'' at the end;

(cc) in clause (ii), by adding ''and'' at the end; and

(dd) by adding at the end the following:

''(iii) in consultation with the Director and the Director of the Cybersecurity and Infrastructure Security Agency, information or information systems used by agencies through shared services, memoranda of understanding, or other agreements;'';

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

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

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

(V) by adding at the end the following:

''(E) not later than 30 days after the date on which an agency system risk assessment is performed under subparagraph (A), providing the assessment to—

''(i) the Director;

''(ii) the Director of the Cybersecurity and Infrastructure Security Agency; and

''(iii) the National Cyber Director;

''(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than annually, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

''(i) be completed considering the agency system risk assessment performed under subparagraph (A); and

''(ii) include a specific evaluation for high value assets; and

"(G) not later than 30 days after completing the evaluation performed under subparagraph (F), providing the evaluation and an implementation plan for using additional cybersecurity procedures determined to be appropriate to—

"(i) the Director of the Cybersecurity and Infrastructure Security Agency;

"(ii) the Director; and

"(iii) the National Cyber Director.";

(ii) in paragraph (2)—

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

(II) in subparagraph (B)—

(aa) by striking "in accordance with standards" and inserting "in accordance with—

"(i) standards"; and

(bb) by adding at the end the following:

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

''(iii) the implementation plan described in paragraph (1)(G);''; and

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

(iii) in paragraph (3)—

(I) in subparagraph (B), by inserting '', in coordination with the Director of the Cybersecurity and Infrastructure Security Agency,'' after ''maintaining'';

(II) in subparagraph (D), by striking ''and'' at the end;

(III) in subparagraph (E), by adding ''and'' at the end; and

(IV) by adding at the end the following:

''(F) implementing mechanisms for using verification specifications, or alternate verification specifications validated by the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Direc-

tor of the National Institute of Standards and Technology, to automatically verify the implementation of standards of agency systems promulgated under section 11331 of title 40 or any additional cybersecurity procedures, as applicable;''; and

(iv) in paragraph (5), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' before ''on the effectiveness'';

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:

''(1) pursuant to subsection (a)(1)(A), performing an agency system risk assessment, which shall include using automated tools consistent with standards, verification specifications, and guidelines promulgated under section 11331 of title 40, as applicable;'';

(ii) in paragraph (2)(D)—

(I) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively;

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

"(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3553 of title 44;"; and

(III) in clause (iv), as so redesignated, by striking "as determined by the agency; and" and inserting "as determined by the agency—

"(I) in coordination with the Director of the Cybersecurity and Infrastructure Security Agency; and

"(II) in consideration of—

"(aa) the agency risk assessment performed under subsection (a)(1)(A); and

"(bb) the determinations of applying more stringent standards and additional cybersecurity procedures pursuant to section 11331(c)(1) of title 40; and";

(iii) in paragraph (5)—

(I) in subparagraph (A), by inserting ", including penetration test-

ing, as appropriate,'' after ''shall include testing''; and

(II) in subparagraph (C), by inserting '', verification specifications,'' after ''with standards'';

(iv) in paragraph (6), by striking ''planning, implementing, evaluating, and documenting'' and inserting ''planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting'';

(v) by redesignating paragraphs (7) and (8) as paragraphs (9) and (10), respectively;

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

''(7) a process for providing the status of every remedial action and known system vulnerability to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;

''(8) a process for providing the verification of the implementation of standards promulgated under

section 11331 of title 40 using verification specifications, automation, and machine-readable data, to the Director and the Director of the Cybersecurity and Infrastructure Security Agency;''; and

(vii) in paragraph (9)(C), as so redesignated—

(I) by striking clause (ii) and inserting the following:

''(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3594;'';

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

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

''(iii) performing the notifications and other activities required under subchapter IV of this title; and''; and

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

(aa) in subclause (I), by striking ''and relevant Offices of Inspector General'';

(bb) in subclause (II), by adding "and" at the end;

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

(i) in paragraph (1)—

(I) in subparagraph (A)—

(aa) in the matter preceding clause (i), by striking "on the adequacy and effectiveness of information security policies, procedures, and practices, including" and inserting "that includes"; and

(bb) in clause (ii), by inserting "unless the Director issues a waiver to the agency under subparagraph (B)(iii)," before "the total number"; and

(II) by striking subparagraph (B) and inserting the following:

"(B) INCIDENT REPORTING WAIVER.—

"(i) CERTIFICATION OF AGENCY INFORMATION SHARING.—If the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, determines that an agency shares any information relating to any incident pursuant to section 3594(a), the Director shall certify that the agency is in compliance with that section.

"(ii) CERTIFICATION OF ISSUING REPORT.—If the Director determines that the Director of the Cybersecurity and Infrastructure Security Agency uses the information described in clause (i) with respect to a particular agency to submit to Congress an annex required under section 3597(e)(3) for that agency, the Director shall certify that the Cybersecurity and Infrastructure Security Agency is in compliance with that section with respect to that agency.

"(iii) WAIVER.—The Director may waive the reporting requirement with respect to the information required to be in-

cluded in the report under subparagraph (A)(ii) for a particular agency if—

"(I) the Director has issued a certification for the agency under clause (i); and

"(II) the Director has issued a certification with respect to the annex of the agency under clause (ii).

"(iv) REVOCATION OF WAIVER OR CERTIFICATIONS.—

"(I) WAIVER.—If, at any time, the Director determines that the Director of the Cybersecurity and Infrastructure Security Agency cannot submit to Congress an annex for a particular agency under section 3597(e)(3)—

"(aa) any waiver previously issued under clause (iii) with respect to that agency shall be considered void; and

"(bb) the Director shall revoke the certification for the annex of that agency under clause (ii).

"(II) CERTIFICATIONS.—If, at any time, the Director determines that an agency has not provided to the Director of the Cybersecurity and Infrastructure Security Agency the totality of incident information required under section 3594(a)—

"(aa) any waiver previously issued under clause (iii) with respect to that agency shall be considered void; and

"(bb) the Director shall revoke the certification for that agency under clause (i).

"(III) REISSUANCE.—If the Director revokes a waiver under this clause, the Director may issue a subsequent waiver if the Director issues new certifications under clauses (i) and (ii).";

(ii) by redesignating paragraphs (2) through (5) as paragraphs (4) through (7), respectively; and

(iii) by inserting after paragraph (1) the following:

"(2) BIANNUAL REPORT.—Not later than 180 days after the date on which an agency completes an agency system risk assessment under subsection (a)(1)(A) and not less frequently than every 2 years, each agency shall submit to the Director, the Secretary, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

"(A) summarizes the agency system risk assessment performed under subsection (a)(1)(A);

"(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the system risk assessment performed under subsection (a)(1)(A); and

"(C) summarizes the evaluations and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether

those evaluations and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency.

''(3) UNCLASSIFIED REPORTS.—Each report submitted under paragraphs (1) and (2)—

''(A) shall be, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

''(B) may include a classified annex.''; and

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' after ''the Director'';

(4) in section 3555—

(A) in subsection (a)(2)(A), by inserting '', including by penetration testing and analyzing the vulnerability disclosure program of the agency'' after ''information systems'';

(B) by striking subsection (f) and inserting the following:

''(f) PROTECTION OF INFORMATION.—(1) Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security.

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

''(3) With respect to information that is not related to national security systems, agencies and evaluators shall make a summary of the information unclassified and publicly available, including information that does not identify—

''(A) specific information system incidents; or

''(B) specific information system vulnerabilities.'';

(C) in subsection (g)(2)—

(i) by striking ''this subsection shall'' and inserting ''this subsection—

''(A) shall'';

(ii) in subparagraph (A), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(B) identify any entity that performs an independent audit under subsection (b).''; and

(D) in subsection (j), by striking ''the Secretary'' and inserting ''the Director of the

~~Cyber Security and Infrastructure Security Agency''; and~~

~~(5) in section 3556(a)—~~

~~(A) in the matter preceding paragraph (1), by inserting ''within the Cybersecurity and Infrastructure Security Agency'' after ''incident center''; and~~

~~(B) in paragraph (4), by striking ''3554(b)'' and inserting ''3554(a)(1)(A)''.~~

~~(d) FEDERAL SYSTEM INCIDENT RESPONSE.—~~

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

~~''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE~~

~~''§ 3591. Definitions~~

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

~~''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:~~

~~''(1) APPROPRIATE NOTIFICATION ENTITIES.—The term 'appropriate notification entities' means—~~

~~''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;~~

"(B) the Committee on Oversight and Reform of the House of Representatives;

"(C) the Committee on Homeland Security of the House of Representatives;

"(D) the appropriate authorization and appropriations committees of Congress;

"(E) the Director;

"(F) the Director of the Cybersecurity and Infrastructure Security Agency;

"(G) the National Cyber Director; and

"(H) the Comptroller General of the United States.

"(2) CONTRACTOR.—The term 'contractor'—

"(A) means any person or business that collects or maintains information that includes personally identifiable information or sensitive personal information on behalf of an agency; and

"(B) includes any subcontractor of a person or business described in subparagraph (A).

"(3) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(4) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means a consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

''(5) VULNERABILITY DISCLOSURE.—The term 'vulnerability disclosure' means a vulnerability identified under section 3559B.

''§ 3592. Notification of high risk exposure after major incident

''(a) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after an agency has a reasonable basis to conclude that a major incident has occurred due to a high risk exposure of personal identifiable information, as described in section 3598(c)(2), the head of the agency shall provide notice of the major incident in accordance with subsection (b) in writing to the last known home mailing address of each individual whom the major incident may have impacted.

''(b) CONTENTS OF NOTICE.—Each notice to an individual required under subsection (a) shall include—

''(1) a description of the rationale for the determination that the major incident resulted in a high

risk of exposure of the personal information of the individual;

''(2) an assessment of the type of risk the individual may face as a result of an exposure;

''(3) contact information for the Federal Bureau of Investigation or other appropriate entity;

''(4) the contact information of each nationwide consumer reporting agency;

''(5) the contact information for questions to the agency, including a telephone number, e-mail address, and website;

''(6) information on any remedy being offered by the agency;

''(7) consolidated Federal Government recommendations on what to do in the event of a major incident; and

''(8) any other appropriate information as determined by the head of the agency.

''(c) DELAY OF NOTIFICATION.—

''(1) IN GENERAL.—The Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security may impose a delay of a notification required under subsection (a) if the notification would disrupt a law enforcement investigation, en-

danger national security, or hamper security remediation actions.

''(2) DOCUMENTATION.—

''(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the head of the agency, the Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Office of Inspector General of the agency that experienced the major incident.

''(B) CONTENTS.—A statement required under subparagraph (A) shall include a written statement from the entity that delayed the notification explaining the need for the delay.

''(C) FORM.—The statement required under subparagraph (A) shall be unclassified, but may include a classified annex.

''(3) RENEWAL.—A delay under paragraph (1) shall be for a period of 2 months and may be renewed.

''(d) UPDATE NOTIFICATION.—If an agency determines there is a change in the reasonable basis to conclude that a major incident occurred, or that there is a change in the details of the information provided to impacted individuals as described in subsection (b), the agency shall as

expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify all such individuals who received a notification pursuant to subsection (a) of those changes.

"(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

"(1) the Director from issuing guidance regarding notifications or the head of an agency from sending notifications to individuals impacted by incidents not determined to be major incidents; or

"(2) the Director from issuing guidance regarding notifications of major incidents or the head of an agency from issuing notifications to individuals impacted by major incidents that contain more information than described in subsection (b).

"§ 3593. Congressional notifications and reports

"(a) INITIAL REPORT.—

"(1) IN GENERAL.—Not later than 5 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency shall submit a written notification and, to the extent practicable, provide a briefing, to the appropriate notification entities, taking into account—

"(A) the information known at the time of the notification;

"(B) the sensitivity of the details associated with the major incident; and

"(C) the classification level of the information contained in the notification.

"(2) CONTENTS.—A notification required under paragraph (1) shall include—

"(A) a summary of the information available about the major incident, including how the major incident occurred, based on information available to agency officials as of the date on which the agency submits the report;

"(B) if applicable, an estimate of the number of individuals impacted by the major incident, including an assessment of the risk level to impacted individuals based on the guidance promulgated under section 3598(c)(1) and any information available to agency officials on the date on which the agency submits the report;

"(C) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exemption to notification granted under subsection (c) or (d) of section 3592; and

"(D) if applicable, an assessment of the impacts to the agency, the Federal Government, or the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

"(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 45 days after the date on which additional information relating to a major incident for which an agency submitted a written notification under subsection (a) is discovered by the agency, the head of the agency shall submit to the appropriate notification entities updates to the written notification that include summaries of—

"(1) the threats and threat actors, vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

"(2) any risk assessment and subsequent risk-based security implementation of the affected information system before the date on which the major incident occurred;

"(3) the status of compliance of the affected information system with applicable security requirements at the time of the major incident;

"(4) an estimate of the number of individuals affected by the major incident based on information available to agency officials as of the date on which the agency submits the update;

"(5) an update to the assessment of the risk of harm to impacted individuals affected by the major incident based on information available to agency officials as of the date on which the agency submits the update;

"(6) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident based on information available to agency officials as of the date on which the agency submits the update; and

"(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d) and status updates on the notification process described in section 3592(a), including any delay or exemption described in subsection (c) or (d), respectively, of section 3592, if applicable.

"(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding

of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written notification under subsection (a), the agency shall provide an updated report to the appropriate notification entities that includes information relating to the change in understanding.

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

''(e) DELAY AND EXEMPTION REPORT.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

''(f) REPORT DELIVERY.—Any written notification or report required to be submitted under this section may be submitted in a paper or electronic format.

''(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

''(1) the ability of an agency to provide additional reports or briefings to Congress; or

‘‘(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

‘‘(h) BINDING OPERATIONAL DIRECTIVE.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under section 3553, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, each agency shall provide to the appropriate notification entities the status of the implementation of the binding operational directive at the agency.

‘‘§ 3594. Government information sharing and incident response

‘‘(a) IN GENERAL.—

‘‘(1) INCIDENT REPORTING.—The head of each agency shall provide any information relating to any incident, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget.

‘‘(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall—

‘‘(A) include detailed information about the safeguards that were in place when the incident occurred;

‘‘(B) whether the agency implemented the safeguards described in subparagraph (A) correctly; and

‘‘(C) in order to protect against a similar incident, identify—

‘‘(i) how the safeguards described in subparagraph (A) should be implemented differently; and

‘‘(ii) additional necessary safeguards.

‘‘(b) COMPLIANCE.—The information provided under subsection (a) shall—

‘‘(1) take into account the level of classification of the information and any information sharing limitations relating to law enforcement; and

‘‘(2) be in compliance with the requirements limiting the release of information under section 552a of title 5 (commonly known as the ‘Privacy Act of 1974’).

‘‘(c) RESPONDING TO INFORMATION REQUESTS FROM AGENCIES EXPERIENCING INCIDENTS.—An agency that receives a request from another agency or Federal entity for information specifically intended to assist in the

remediation or notification requirements due to an incident shall provide that information to the greatest extent possible, in accordance with guidance issued by the Director and taking into account classification, law enforcement, national security, and compliance with section 552a of title 5 (commonly known as the 'Privacy Act of 1974').

''(d) INCIDENT RESPONSE.—Each agency that has a reasonable basis to conclude that a major incident occurred, regardless of delays from notification granted for a major incident, shall consult with the Cybersecurity and Infrastructure Security Agency regarding—

''(1) incident response and recovery; and

''(2) recommendations for mitigating future incidents.

"§ 3595. Responsibilities of contractors and grant recipients

''(a) NOTIFICATION.—

''(1) IN GENERAL.—Subject to paragraph (3), any contractor of an agency or recipient of a grant from an agency that has a reasonable basis to conclude that an incident involving Federal information has occurred shall immediately notify the agency.

''(2) PROCEDURES.—

''(A) MAJOR INCIDENT.—Following notification of a major incident by a contractor or re-

cipient of a grant under paragraph (1), an agency, in consultation with the contractor or grant recipient, as applicable, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

"(B) INCIDENT.—Following notification of an incident by a contractor or recipient of a grant under paragraph (1), an agency, in consultation with the contractor or grant recipient, as applicable, shall carry out the requirements under section 3594 with respect to the incident.

"(3) APPLICABILITY.—This subsection shall apply to a contractor of an agency or a recipient of a grant from an agency that—

"(A) receives information from the agency that the contractor or recipient, as applicable, is not contractually authorized to receive;

"(B) experiences an incident relating to Federal information on an information system of the contractor or recipient, as applicable; or

"(C) identifies an incident involving a Federal information system.

"(b) INCIDENT RESPONSE.—Any contractor of an agency or recipient of a grant from an agency that has a reasonable basis to conclude that a major incident oc-

curred shall, in coordination with the agency, consult with the Cybersecurity and Infrastructure Security Agency regarding—

"(1) incident response assistance; and

"(2) recommendations for mitigating future incidents at the agency.

"(c) EFFECTIVE DATE.—This section shall apply on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2021.

"§ 3596. Training

"(a) IN GENERAL.—Each agency shall develop training for individuals at the agency with access to Federal information or information systems on how to identify and respond to an incident, including—

"(1) the internal process at the agency for reporting an incident; and

"(2) the obligation of the individual to report to the agency a confirmed major incident and any suspected incident, involving information in any medium or form, including paper, oral, and electronic.

"(b) APPLICABILITY.—The training developed under subsection (a) shall—

~~"(1) be required for an individual before the individual may access Federal information or information systems; and~~

~~"(2) apply to individuals with temporary access to Federal information or information systems, such as detailees, contractors, subcontractors, grantees, volunteers, and interns.~~

~~"(c) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (a) may be included as part of an annual privacy or security awareness training of the agency, as applicable.~~

~~"§ 3597. Analysis and report on Federal incidents~~

~~"(a) DEFINITION OF COMPROMISE.—In this section, the term 'compromise' means—~~

~~"(1) an incident;~~

~~"(2) a result of a penetration test in which the tester successfully gains access to a system within the standards under section 3559A;~~

~~"(3) a vulnerability disclosure; or~~

~~"(4) any other event that the Director of the Cybersecurity and Infrastructure Security Agency determines identifies an exploitable vulnerability in an agency system.~~

~~"(b) ANALYSIS OF FEDERAL INCIDENTS.—~~

"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall perform continuous monitoring of compromises of agencies.

"(2) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall develop and perform continuous monitoring and quantitative and qualitative analyses of compromises of agencies, including—

"(A) the causes of successful compromises, including—

"(i) attacker tactics, techniques, and procedures; and

"(ii) system vulnerabilities, including zero days, unpatched systems, and information system misconfigurations;

"(B) the scope and scale of compromises of agencies;

"(C) cross Federal Government root causes of compromises of agencies;

"(D) agency response, recovery, and remediation actions and effectiveness of incidents, as applicable; and

"(E) lessons learned and recommendations in responding, recovering, remediating, and mitigating future incidents.

"(3) AUTOMATED ANALYSIS.—The analyses developed under paragraph (2) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

"(4) SHARING OF DATA AND ANALYSIS.—

"(A) IN GENERAL.—The Director shall share on an ongoing basis the analyses required under this subsection with agencies to—

"(i) improve the understanding of agencies with respect to risk; and

"(ii) support the cybersecurity improvement efforts of agencies.

"(B) FORMAT.—In carrying out subparagraph (A), the Director shall share the analyses—

"(i) in human-readable written products; and

"(ii) to the greatest extent practicable, in machine-readable formats in order to enable automated intake and use by agencies.

"(c) ANNUAL REPORT ON FEDERAL COMPROMISES.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall submit to the appropriate notification entities a report that includes—

"(1) a summary of causes of compromises from across the Federal Government that categorizes those compromises by the items described in paragraphs (1) through (4) of subsection (a);

"(2) the quantitative and qualitative analyses of compromises developed under subsection (b)(2) on an agency-by-agency basis and comprehensively; and

"(3) an annex for each agency that includes the total number of compromises of the agency and categorizes those compromises by the items described in paragraphs (1) through (4) of subsection (a).

"(d) PUBLICATION.—A version of each report submitted under subsection (c) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

"(e) INFORMATION PROVIDED BY AGENCIES.—The analysis required under subsection (b) and each report

submitted under subsection (c) shall utilize information provided by agencies pursuant to section 3594(d).

''(f) REQUIREMENT TO ANONYMIZE INFORMATION.—In publishing the public report required under subsection (d), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently anonymize and compile information such that no specific incidents of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

''§ 3598. Major incident guidance

''(a) IN GENERAL.—Not later than 90 days after the date of enactment of the Federal Information Security Management Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

''(b) REQUIREMENTS.—With respect to the guidance issued under subsection (a), the definition of the term 'major incident' shall—

''(1) include, with respect to any information collected or maintained by or on behalf of an agency or an information system used or operated by an

agency or by a contractor of an agency or another organization on behalf of an agency—

"(A) any incident the head of the agency determines is likely to have an impact on the national security, homeland security, or economic security of the United States;

"(B) any incident the head of the agency determines is likely to have an impact on the operations of the agency, a component of the agency, or the Federal Government, including an impact on the efficiency or effectiveness of agency information systems;

"(C) any incident that the head of an agency, in consultation with the Chief Privacy Officer of the agency, determines involves a high risk incident in accordance with the guidance issued under subsection (c)(1);

"(D) any incident that involves the unauthorized disclosure of personally identifiable information of not less than 500 individuals, regardless of the risk level determined under the guidance issued under subsection (c)(1);

"(E) any incident the head of the agency determines involves a high value asset owned or operated by the agency; and

"(F) any other type of incident determined appropriate by the Director;

"(2) stipulate that every agency shall be considered to have experienced a major incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident that occurs at not less than 2 agencies—

"(A) is enabled by a common technical root cause, such as a supply chain compromise, a common software or hardware vulnerability; or

"(B) is enabled by the related activities of a common actor; and

"(3) stipulate that, in determining whether an incident constitutes a major incident because that incident—

"(A) is any incident described in paragraph (1), the head of an agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency;

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

"(C) is an incident described in subparagraph (C) or (D) of paragraph (1), the head of the agency shall consult with—

"(i) the Privacy and Civil Liberties Oversight Board; and

"(ii) the Executive Director of the Federal Trade Commission.

"(c) GUIDANCE ON RISK TO INDIVIDUALS.—

"(1) IN GENERAL.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, the Privacy and Civil Liberties Oversight Board, and the Executive Director of the Federal Trade Commission, shall develop and issue guidance to agencies that establishes a risk-based framework for determining the level of risk that an incident involving personally identifiable information could result in substantial harm, physical harm, embarrassment, or unfairness to an individual.

"(2) RISK LEVELS AND CONSIDERATIONS.—The risk-based framework included in the guidance issued under paragraph (1) shall—

"(A) include a range of risk levels, including a high risk level; and

"(B) consider—

"(i) any personally identifiable information that was exposed as a result of an incident;

"(ii) the circumstances under which the exposure of personally identifiable information of an individual occurred; and

"(iii) whether an independent evaluation of the information affected by an incident determines that the information is unreadable, including, as appropriate, instances in which the information is—

"(I) encrypted; and

"(II) determined by the Director of the Cybersecurity and Infrastructure Security Agency to be of sufficiently low risk of exposure.

"(3) APPROVAL.—

"(A) IN GENERAL.—The guidance issued under paragraph (1) shall include a process by which the Director, jointly with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, may approve

the designation of an incident that would be considered high risk as lower risk if information exposed by the incident is unreadable, as described in paragraph (2)(B)(iii).

''(B) DOCUMENTATION.—The Director shall report any approval of an incident granted by the Director under subparagraph (A) to—

''(i) the head of the agency that experienced the incident;

''(ii) the inspector general of the agency that experienced the incident; and

''(iii) the Director of the Cybersecurity and Infrastructure Security Agency.

''(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

''(1) an update, if necessary, to the guidance issued under subsections (a) and (c);

''(2) the definition of the term 'major incident' included in the guidance issued under subsection (a);

"(3) an explanation of, and the analysis that led to, the definition described in paragraph (2); and

"(4) an assessment of any additional datasets or risk evaluation criteria that should be included in the risk-based framework included in the guidance issued under subsection (c)(1).".

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

"SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

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

(a) INFORMATION TECHNOLOGY MODERNIZATION CENTERS OF EXCELLENCE PROGRAM ACT.—Section 2(c)(4)(A)(ii) of the Information Technology Modernization Centers of Excellence Program Act (40 U.S.C. 11301 note) is amended by striking the period at the end and inserting ", which shall be provided in coordination with the Director of the Cybersecurity and Infrastructure Security Agency.".

(b) MODERNIZING GOVERNMENT TECHNOLOGY.—Subtitle G of title X of Division A of the National Defense

~~Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note) is amended—~~

~~(1) in section 1077(b)—~~

~~(A) in paragraph (5)(A), by inserting "improving the cybersecurity of systems and" before "cost savings activities"; and~~

~~(B) in paragraph (7)—~~

~~(i) in the paragraph heading, by striking "CIO" and inserting "CIO";~~

~~(ii) by striking "In evaluating projects" and inserting the following:~~

~~"(A) CONSIDERATION OF GUIDANCE.—In evaluating projects";~~

~~(iii) in subparagraph (A), as so designated, by striking "under section 1094(b)(1)" and inserting "guidance issued by the Director"; and~~

~~(iv) by adding at the end the following:~~

~~"(B) CONSULTATION.—In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency."; and~~

~~(2) in section 1078—~~

(A) by striking subsection (a) and inserting the following:

''(a) DEFINITIONS.—In this section:

''(1) AGENCY.—The term 'agency' has the meaning given the term in section 551 of title 5, United States Code.

''(2) HIGH VALUE ASSET.—The term 'high value asset' has the meaning given the term in section 3552 of title 44, United States Code.'';

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

''(8) PROPOSAL EVALUATION.—The Director shall—

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

''(B) require that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a chain risk management plan, to be reviewed by the member of the Technology Modernization Board described in subsection (c)(5)(C).''; and

(C) in subsection (c)—

(i) in paragraph (2)(A)(i), by inserting '', including a consideration of the im-

pact on high value assets'' after ''operational risks'';

(ii) in paragraph (5)—

(I) in subparagraph (A), by striking ''and'' at the end;

(II) in subparagraph (B), by striking the period at the end and inserting ''and''; and

(III) by adding at the end the following:

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

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

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

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''use, and disposal, and, in coordination with the Director of the Cybersecurity and Infrastructure Secu-

rity Agency, promote and improve the security, of'';

(B) in subsection (c)—

(i) in paragraph (2), by inserting ''in consultation with the Director of the Cybersecurity and Infrastructure Security Agency'' before '', and results of'';

(ii) in paragraph (3)—

(I) in subparagraph (A), by striking '', and performance'' and inserting ''security, and performance''; and

(II) in subparagraph (C)—

(aa) by striking ''For each major'' and inserting the following:

''(i) IN GENERAL.—For each major''; and

(bb) by adding at the end the following:

''(ii) CYBERSECURITY.—In categorizing an investment according to risk under clause (i), the Chief Information Officer of the covered agency shall consult with the Director of the Cybersecurity and

Infrastructure Security Agency on the cybersecurity or supply chain risk.

''(iii) SECURITY RISK GUIDANCE.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance for the categorization of an investment under clause (i) according to the cybersecurity or supply chain risk.''; and

(iii) in paragraph (4)—

(I) in subparagraph (A)—

(aa) in clause (ii), by striking ''and'' at the end;

(bb) in clause (iii), by striking the period at the end and inserting ''; and''; and

(cc) by adding at the end the following:

''(iv) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the cybersecurity risks of the investment.''; and

(II) in subparagraph (B), in the matter preceding clause (i), by inserting ''not later than 30 days after the

date on which the review under subparagraph (A) is completed,'' before ''the Administrator'';

(C) in subsection (f)—

(i) by striking ''heads of executive agencies to develop'' and inserting ''heads of executive agencies to—

''(1) develop'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(2) consult with the Director of the Cybersecurity and Infrastructure Security Agency for the development and use of supply chain security best practices.''; and

(D) in subsection (h), by inserting '', including cybersecurity performances,'' after ''the performances''; and

(2) in section 11303(b)(2)(B)—

(A) in clause (i), by striking ''or'' at the end;

(B) in clause (ii), by adding ''or'' at the end; and

(C) by adding at the end the following:

"(iii) whether the function should be performed by a shared service offered by another executive agency;".

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

(1) in section 11312(a), by inserting ", including security risks" after "managing the risks";

(2) in section 11313(1), by striking "efficiency and effectiveness" and inserting "efficiency, security, and effectiveness";

(3) in section 11317, by inserting "security," before "or schedule"; and

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

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

(1) in subsection (a), by striking "section 3532(b)(1)" and inserting "section 3552(b)";

(2) in subsection (b)(1)(A)—

(A) by striking "in consultation" and inserting "in coordination";

(B) by striking "the Secretary of Homeland Security" and inserting "the Director of

the Cybersecurity and Infrastructure Security Agency'', and

(C) by inserting ''and associated verification specifications developed under subsection (g)'' before ''pertaining to Federal'';

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

''(c) APPLICATION OF MORE STRINGENT STANDARDS.—

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

''(A) evaluate the need to employ standards for cost-effective, risk-based information security for all systems, operations, and assets within or under the supervision of the agency that are more stringent than the standards promulgated by the Director under this section, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

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

"(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ more stringent standards under paragraph (1), the head of an agency shall consider available risk information, including—

"(A) the status of cybersecurity remedial actions of the agency;

"(B) any vulnerability information relating to agency systems that is known to the agency;

"(C) incident information of the agency;

"(D) information from—

"(i) penetration testing performed under section 3559A of title 44; and

"(ii) information from the verification disclosure program established under section 3559B of title 44;

"(E) agency threat hunting results under section 207 of the Federal Information Security Modernization Act of 2021;

"(F) Federal and non-Federal threat intelligence;

"(G) data on compliance with standards issued under this section, using the verification specifications developed under subsection (f) when appropriate;

''(H) agency system risk assessments of the agency performed under section 3554(a)(1)(A) of title 44; and

''(I) any other information determined relevant by the head of the agency.'';

(4) in subsection (d)(2)—

(A) by striking the paragraph heading and inserting ''CONSULTATION, NOTICE, AND COMMENT'';

(B) by inserting ''promulgate,'' before ''significantly modify''; and

(C) by striking ''shall be made after the public is given an opportunity to comment on the Director's proposed decision.'' and inserting ''shall be made—

''(A) for a decision to significantly modify or not promulgate such a proposed standard, after the public is given an opportunity to comment on the Director's proposed decision;

''(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council

of the Inspectors General on Integrity and Efficiency;

''(C) considering the Federal risk assessments performed under section 3553(i) of title 44; and

''(D) considering the extent to which the proposed standard reduces risk relative to the cost of implementation of the standard.''; and

(5) by adding at the end the following:

''(e) REVIEW OF PROMULGATED STANDARDS.—

''(1) IN GENERAL.—Not less frequently than once every 2 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the standards in effect promulgated under this section in reducing cybersecurity risks and determine whether any changes to those standards are appropriate based on—

''(A) the Federal risk assessment developed under section 3553(i) of title 44;

''(B) public comment; and

"(C) an assessment of the extent to which the proposed standards reduce risk relative to the cost of implementation of the standards.

"(2) UPDATED GUIDANCE.—Not later than 90 days after the date of the completion of the review under paragraph (1), the Director of the Office of Management and Budget shall issue guidance to agencies to make any necessary updates to the standards in effect promulgated under this section based on the results of the review.

"(3) CONGRESSIONAL REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report that includes—

"(A) the review of the standards in effect promulgated under this section conducted under paragraph (1);

"(B) the risk mitigation offered by each standard described in subparagraph (A); and

"(C) a summary of—

''(i) the standards to which changes were determined appropriate during the review; and

''(ii) anticipated changes to the standards under this section in guidance issued under paragraph (2).

''(f) VERIFICATION SPECIFICATIONS.—Not later than 1 year after the date on which the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director of the National Institute of Standards and Technology, as practicable, shall develop technical specifications to enable the automated verification of the implementation of the controls within the standard.''.

SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

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

(1) RECOMMENDATIONS.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Secu-

rity Agency, in coordination with the Chair of the Federal Trade Commission, the Chair of the Securities and Exchange Commission, the Secretary of the Treasury, the Director of the Federal Bureau of Investigation, the Director of the National Institute of Standards and Technology, and the head of any other appropriate Federal or non-Federal entity, shall consolidate, maintain, and make publicly available recommendations for individuals whose personal information, as defined in section 3591 of title 44, United States Code, as added by this Act, is inappropriately exposed as a result of a high risk incident described in section 3598(c)(2) of title 44, United States Code.

(2) PLAN FOR ANALYSIS OF, AND REPORT ON, FEDERAL INCIDENTS.—

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

(i) develop a plan for the development of the analysis required under section 3597(b) of title 44, United States Code, as added by this Act, and the report required

under subsection (c) of that section that includes—

(I) a description of any challenges the Director anticipates encountering; and

(II) the use of automation and machine-readable formats for collecting, compiling, monitoring, and analyzing data; and

(ii) provide to the appropriate congressional committees a briefing on the plan developed under clause (i).

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

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

(ii) the development of the report required under section 3597(c) of title 44, United States Code, as added by this Act.

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

(1) FISMA.—Section 2 of the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554 note) is amended—

(A) by striking subsection (b); and

(B) by redesignating subsections (c) through (f) as subsections (b) through (e), respectively.

(2) INCIDENT DATA SHARING.—

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

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

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

(I) the causes of incidents;

(II) the scope and scale of incidents within the agency networks and systems;

(III) cross Federal Government root causes of incidents;

(IV) agency response, recovery, and remediation actions; and

(V) the effectiveness of incidents;

(ii) enable the efficient development of—

(I) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

(II) the report on Federal compromises required under section 3597(c) of title 44, United States Code, as added by this Act;

(iii) include requirements for the timeliness of data production; and

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

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 3594(c) of title 44, United States Code, as added by this Act, to provide information to other agencies experiencing incidents.

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this Act.

(5) CONTRACTOR AND GRANTEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict existing regulations, policies, and procedures relating to the responsibilities of contractors and grant recipients established under section 3595 of title 44, United States Code, as added by this Act.

(B) EXISTING PROCESSES.—To the greatest extent practicable, the guidance issued

under subparagraph (A) shall allow contractors and grantees to use existing processes for notifying Federal agencies of incidents involving information of the Federal Government.

(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).

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

(1) in paragraph (11), by striking "or" at the end;

(2) in paragraph (12), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.".

SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

(1) completing the agency system risk assessment required under section 3554(a)(1)(A) of title 44, United States Code, as amended by this Act;

(2) implementing additional cybersecurity procedures, which shall include resources for shared services;

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44, United States Code, as amended by this Act, to the Director and the Cybersecurity and Infrastructure Security Agency using automation and machine-readable data, as practicable, which shall include—

(A) specific standards for the automation and machine-readable data; and

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

(4) interpreting the definition of ''high value asset'' in section 3552 of title 44, United States Code, as amended by this Act;

(5) implementing standards in agency authorization processes to encourage the tailoring of processes to agency and system risk that are proportionate to the sensitivity of systems, which shall include—

(A) a clarification of—

(i) the acceptable use and development of customization of standards promulgated under section 11331 of title 40, United States Code; and

(ii) the acceptable use of risk-based authorization procedures authorized on the date of enactment of this Act; and

(B) a requirement to coordinate with Inspectors Generals of agencies to ensure consistent understanding and application of agency policies for the purpose of Inspector General audits; and

(6) requiring, as practicable and pursuant to section 203, an evaluation of agency cybersecurity using metrics that are—

(A) based on outcomes; and

(B) based on time.

SEC. 105. AGENCY REQUIREMENTS TO NOTIFY ENTITIES IMPACTED BY INCIDENTS.

Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance that requires agencies to notify entities that are compelled to share sensitive information with the agency of an incident that impacts—

(1) sensitive information shared with the agency by the entity; or

(2) the systems used to the transmit sensitive information described in paragraph (1) to the agency.

TITLE II—IMPROVING FEDERAL CYBERSECURITY

SEC. 201. EVALUATION OF EFFECTIVENESS OF STANDARDS.

(a) IN GENERAL.—As a component of the evaluation and report required under section 3555(h) of title 44, United States Code, and not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study that—

(1) assesses the standards promulgated under section 11331(b) of title 40, United States Code to determine the degree to which agencies use the authority under section 11331(c)(1) of title 40, United States Code to customize the standards relative to the risks facing each agency and agency system;

~~(2) assesses the effectiveness of the standards described in paragraph (1), including any standards customized by agencies under section 11331(c)(1) of title 40, United States Code, at improving agency cybersecurity;~~

~~(3) examines the quantification of cybersecurity risk in the private sector for any applicability for use by the Federal Government;~~

~~(4) examines cybersecurity metrics existing as of the date of enactment of this Act used by the Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the heads of other agencies to evaluate the effectiveness of information security policies and practices; and~~

~~(5) with respect to the standards described in paragraph (1), provides recommendations for—~~

~~(A) the addition or removal of standards; or~~

~~(B) the customization of—~~

~~(i) the standards by agencies under section 11331(c)(1) of title 40, United States Code; or~~

~~(ii) specific controls within the standards.~~

(b) INCORPORATION OF STUDY.—The Director shall incorporate the results of the study performed under subsection (a) into the review of standards required under section 11331(c) of title 40, United States Code.

(c) BRIEFING.—Not later than 30 days after the date on which the study performed under subsection (a) is completed, the Comptroller General of the United States shall provide to the appropriate congressional committees a briefing on the study.

SEC. 202. MOBILE SECURITY STANDARDS.

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

(1) evaluate mobile application security standards promulgated under section 11331(b) of title 44, United States Code; and

(2) issue guidance to implement mobile security standards in effect on the date of enactment of this Act promulgated under section 11331(b) of title 40, United States Code, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

(1) a requirement, pursuant to section 3506(b)(4) of title 44, United States Code, for every

agency to maintain a continuous inventory of every—

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

(B) mobile application installed on a mobile device described in subparagraph (A); and

(C) vulnerability identified by the agency associated with a mobile device or mobile application described in subparagraphs (A) and (B); and

(2) a requirement for every agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(C) and other risks.

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies for sharing the inventory of the agency required under subsection (b)(1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

(d) BRIEFING.—Not later than 60 days after the date on which the Director issues guidance under subsection (a)(2), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency,

shall provide to the appropriate congressional committees a briefing on the guidance.

SEC. 203. QUANTITATIVE CYBERSECURITY METRICS.

(a) ESTABLISHING TIME-BASED METRICS.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(A) update the metrics used to measure security under section 3554 of title 44, United States Code, including any metrics developed pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)), to include standardized metrics to quantitatively evaluate and identify trends in agency cybersecurity performance, including performance for incident response; and

(B) evaluate the metrics described in subparagraph (A).

(2) QUALITIES.—With respect to the updated metrics required under paragraph (1)—

(A) not less than 2 of the metrics shall be time-based; and

(B) the metrics may include other measurable outcomes.

(3) EVALUATION.—The evaluation required under paragraph (1)(B) shall evaluate—

(A) the amount of time it takes for an agency to detect an incident; and

(B) the amount of time that passes between—

(i) the detection and remediation of an incident; and

(ii) the remediation of an incident and the recovery from the incident.

(b) IMPLEMENTATION.—

(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promulgate guidance that requires the use of the updated metrics developed under subsection (a)(1)(A) by every agency over a 4-year period beginning on the date on which the metrics are developed to track trends in the incident response capabilities of agencies.

(2) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), not less than 3 agencies shall be subjected to substantially similar penetration tests in order to

validate the utility of the metrics developed under subsection (a)(1)(A).

(3) DATABASE.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop and use a database that—

(A) stores agency metrics information; and

(B) allows for the performance of cross-agency comparison of agency incident response capability trends.

(c) UPDATED METRICS.—

(1) IN GENERAL.—The Director may issue guidance that updates the metrics developed under subsection (a)(1)(A) if the updated metrics—

(A) have the qualities described in subsection (a)(2); and

(B) can be evaluated under subsection (a)(3).

(2) DATA SHARING.—The guidance issued under paragraph (1) shall require agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency with the updated metrics included in that guidance against the metrics developed under subsection (a)(1)(A).

(d) CONGRESSIONAL REPORTS.—

(1) UPDATED METRICS.—Not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security completes the evaluation required under subsection (a)(1)(B), the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees a report on the updated metrics developed under subsection (a)(1)(A).

(2) PROGRAM.—Not later than 180 days after the date on which guidance is promulgated under subsection (b)(1), the Director shall submit to the appropriate congressional committees a report on the results of the use of the updated metrics developed under subsection (a)(1)(A) by agencies.

SEC. 204. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) RECOMMENDATIONS.—Not later than 60 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General and the National Cyber Director, shall submit to the Director recommendations on requirements for logging events on agency systems and retaining other relevant data within the systems and networks of an agency.

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

(1) the types of logs to be maintained;

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

(3) the time periods for agencies to enable recommended logging and security requirements;

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

(5) requirements to ensure that, upon request, agencies provide logs to—

(A) the Director of the Cybersecurity and Infrastructure Security Agency for a cybersecurity purpose; and

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

(6) ensuring the highest level security operations center of each agency has visibility into all agency logs.

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall promulgate guidance to agencies to establish requirements for logging, log retention, log

~~management, and sharing of log data with other appropriate agencies.~~

~~(d) PERIODIC REVIEW.—Not later than 2 years after the date on which the Director of the Cybersecurity and Infrastructure Security Agency submits the recommendations required under subsection (a), and not less frequently than every 2 years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General, shall evaluate the recommendations and provide an update on the recommendations to the Director as necessary.~~

~~SEC. 205. CISA AGENCY ADVISORS.~~

~~(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 1 cybersecurity professional employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the Chief Information Officer of each agency.~~

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

~~(1) cybersecurity threats facing agencies, including any specific threats to the assigned agency;~~

~~(2) performing risk assessments of agency systems; and~~

(3) other Federal cybersecurity initiatives.

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

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

(2) serving as an incident response point of contact between the assigned agency and the Cybersecurity and Infrastructure Security Agency; and

(3) familiarizing themselves with agency systems, processes, and procedures to better facilitate support to the agency in responding to incidents.

(d) LIMITATION.—An advisor assigned under subsection (a) shall not be a contractor.

(e) MULTIPLE ASSIGNMENTS.—One individual advisor made be assigned to multiple agency Chief Information Officers under subsection (a).

SEC. 206. FEDERAL PENETRATION TESTING POLICY.

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

"§ 3559A. Federal penetration testing

"(a) DEFINITIONS.—In this section:

"(1) AGENCY OPERATIONAL PLAN.—The term 'agency operational plan' means a plan of an agency for the use of penetration testing.

~~"(2) RULES OF ENGAGEMENT.—The term 'rules of engagement' means a set of rules established by an agency for the use of penetration testing.~~

~~"(b) GUIDANCE.—~~

~~"(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance that—~~

~~"(A) requires agencies to use, when and where appropriate, penetration testing on agency systems; and~~

~~"(B) requires agencies to develop an agency operational plan and rules of engagement that meet the requirements under subsection (c).~~

~~"(2) PENETRATION TESTING GUIDANCE.—The guidance issued under this section shall—~~

~~"(A) permit an agency to use, for the purpose of performing penetration testing—~~

~~"(i) a shared service of the agency or another agency; or~~

~~"(ii) an external entity, such as a vendor;~~

~~"(B) include templates and frameworks for reporting the results of penetration testing,~~

without regard to the status of the entity that performs the penetration testing; and

''(C) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, without regard to the status of the entity that performs the penetration testing.

''(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

''(1) require the agency to perform penetration testing on the high value assets of the agency;

''(2) establish guidelines for avoiding, as a result of penetration testing—

''(A) adverse impacts to the operations of the agency;

''(B) adverse impacts to operational networks and systems of the agency; and

''(C) inappropriate access to data;

''(3) require the results of penetration testing to include feedback to improve the cybersecurity of the agency; and

''(4) include mechanisms for providing consistently formatted, and, if applicable, automated and

machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

''(d) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) establish a certification process for the performance of penetration testing by both Federal and non-Federal entities that establishes minimum quality controls for penetration testing;

''(2) develop operational guidance for instituting penetration testing programs at agencies;

''(3) develop and maintain a centralized capability to offer penetration testing as a service to Federal and non-Federal entities; and

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

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

''(1) not less frequently than annually, inventory all Federal penetration testing assets; and

''(2) develop and maintain a Federal strategy for the use of penetration testing.

''(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.—

''(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop a framework for prioritizing Federal penetration testing resources among agencies.

''(2) CONSIDERATIONS.—In developing the framework under this subsection, the Director shall consider—

''(A) agency system risk assessments performed under section 3554(a)(1)(A);

''(B) the Federal risk assessment performed under section 3553(i);

''(C) the analysis of Federal incident data performed under section 3597; and

''(D) any other information determined appropriate by the Director or the Director of the Cybersecurity and Infrastructure Security Agency.''.

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

''3559A. Federal penetration testing.''.

(c) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by section 1705 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283) and section 101, is further amended—

(1) in paragraph (8)(B), by striking ''and'' at the end;

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

(3) by inserting after paragraph (8) the following:

''(9) performing penetration testing with or without advance notice to, or authorization from, agencies, to identify vulnerabilities within Federal information systems; and''.

SEC. 207. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall establish a program to provide ongoing, hypothesis-driven threat-hunting services on the network of each agency.

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish the program required under paragraph (1) that describes how the Director of the Cybersecurity and Infrastructure Security Agency plans to—

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

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

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

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

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

(ii) additional cybersecurity procedures under section 3554 of title 44, United States Code.

(b) REPORTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(1) not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security Agency completes the plan required under subsection (a)(2), a report on the plan to provide threat hunting services to agencies;

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program, a report providing any updates to the plan developed under subsection (a)(2); and

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services to agencies other than the Cybersecurity and Infrastructure Security Agency, a report describing lessons learned from providing those services.

SEC. 208. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44 of United States Code is amended by inserting after section 3559A, as added by section 206 of this Act, the following:

"§ 3559B. Federal vulnerability disclosure programs

"(a) DEFINITIONS.—In this section:

"(1) REPORT.—The term 'report' means a vulnerability disclosure made to an agency by a reporter.

"(2) REPORTER.—The term 'reporter' means an individual that submits a vulnerability report pursuant to the vulnerability disclosure process of an agency.

"(b) RESPONSIBILITIES OF OMB.—

"(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that conducts a security research activity that the head of the agency determines—

"(A) represents a good faith effort to follow the vulnerability disclosure policy developed under subsection (d)(2) of the agency; and

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

"(2) SHARING INFORMATION WITH CISA.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the Cybersecurity and Infrastructure Security Agency, including—

"(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on an agency information system that uses commercial software or services;

"(B) information relating to vulnerability disclosure, coordination, or remediation activities of an agency, particularly as those activities relate to outside organizations—

"(i) with which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security can assist; or

"(ii) about which the head of the agency believes the Director of the Cyber-

security and Infrastructure Security should know; and

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

"(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—

"(A) IN GENERAL.—The Director shall issue guidance to agencies on the required minimum scope of agency systems covered by the vulnerability disclosure policy of an agency required under subsection (d)(2).

"(B) DEADLINE.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director shall update the guidance issued under subparagraph (A) to require that every agency system that is connected to the internet is covered by the vulnerability disclosure policy of the agency.

"(c) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) provide support to agencies with respect to the implementation of the requirements of this section;

''(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section; and

''(3) upon a request by an agency, assist the agency in the disclosure to vendors of newly identified vulnerabilities in vendor products and services.

''(d) RESPONSIBILITIES OF AGENCIES.—

''(1) PUBLIC INFORMATION.—The head of each agency shall make publicly available, with respect to each internet domain under the control of the agency that is not a national security system—

''(A) an appropriate security contact; and

''(B) the component of the agency that is responsible for the internet accessible services offered at the domain.

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

''(A) describe—

~~"(i) the scope of the systems of the agency included in the vulnerability disclosure policy;~~

~~"(ii) the type of information system testing that is authorized by the agency;~~

~~"(iii) the type of information system testing that is not authorized by the agency; and~~

~~"(iv) the disclosure policy of the agency for sensitive information;~~

~~"(B) include a provision that authorizes the anonymous submission of a vulnerability by a reporter;~~

~~"(C) with respect to a report to an agency, describe—~~

~~"(i) how the reporter should submit the report; and~~

~~"(ii) if the report is not anonymous under subparagraph (B), when the reporter should anticipate an acknowledgment of receipt of the report by the agency; and~~

~~"(D) include any other relevant information.~~

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

''(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program established under this section.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended

by adding after the item relating to section 3559A the following:

"3559B. Federal vulnerability disclosure programs.".

SEC. 209. IMPLEMENTING PRESUMPTION OF COMPROMISE AND ZERO TRUST ARCHITECTURES.

(a) RECOMMENDATIONS.—Not later than 60 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director of the National Institute of Standards and Technology, shall develop recommendations to increase the internal defenses of agency systems to—

(1) limit the ability of entities that cause incidents to move laterally through or between agency systems;

(2) identify incidents more quickly;

(3) isolate and remove unauthorized entities from agency systems more quickly;

(4) implement zero trust architecture; and

(5) otherwise increase the resource costs for entities that cause incidents; and

(b) OMB GUIDANCE.—Not later than 180 days after the date on which the recommendations under subsection (a) are completed, the Director shall issue guidance to agencies that requires the implementation of the recommendations.

(c) AGENCY IMPLEMENTATION PLANS.—Not later than 60 days after the date on which the Director issues guidance under subsection (b), the head of each agency shall submit to the Director a plan to implement zero trust architecture that includes—

(1) a description of any steps the agency has completed;

(2) an identification of activities that will have the most immediate security impact; and

(3) a schedule to implement the plan.

(d) REPORT AND BRIEFING.—Not later than 90 days after the date on which the Director issues guidance required under subsection (b), the Director shall provide a briefing to the appropriate congressional committees on the guidance and the agency implementation plans submitted under subsection (c).

SEC. 210. AUTOMATION REPORTS.

(a) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of automation under paragraphs (1), (5)(C) and (7)(B) of section 3554(b) of title 44, United States Code.

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

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

SEC. 211. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

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

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 301. CONTINUOUS INDEPENDENT FISMA EVALUATION PILOT.

(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall establish a pilot program to perform continual agency auditing of the standards promulgated under section 11331 of title 40, United States Code.

(b) PURPOSE.—

(1) IN GENERAL.—The purpose of the pilot program established under subsection (a) shall be to

develop the capability to continuously audit agency cybersecurity postures, rather than performing an annual audit.

(2) USE OF INFORMATION.—It is the sense of Congress that information relating to agency cybersecurity postures should be used, on an ongoing basis, to increase agency understanding of cybersecurity risk and improve agency cybersecurity.

(c) PARTICIPATING AGENCIES.—

(1) IN GENERAL.—The Director, in coordination with the Council of the Inspectors General on Integrity and Efficiency and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall identify not less than 1 agency and the Inspector General of each identified agency to participate in the pilot program established under subsection (a).

(2) CAPABILITIES OF AGENCY.—An agency selected under paragraph (1) shall have advanced cybersecurity capabilities, including the capability to implement verification specifications and other automated and machine-readable means of sharing information.

(3) CAPABILITIES OF INSPECTOR GENERAL.—The Inspector General of an agency selected under

paragraph (1) shall have advanced cybersecurity capabilities, including the ability—

(A) to perform real-time or almost real-time and continuous analysis of the use of verification specifications by the agency to assess compliance with standards promulgated under section 11331 of title 40, United States Code; and

(B) to assess the impact and deployment of additional cybersecurity procedures.

(d) DUTIES.—The Director, in coordination with the Council of the Inspectors General on Integrity and Efficiency, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of each agency participating in the pilot program under subsection (c), shall develop processes and procedures to perform a continuous independent evaluation of—

(1) the compliance of the agency with—

(A) the standards promulgated under section 11331 of title 40, United States Code, using verification specifications to the greatest extent practicable; and

(B) any additional cybersecurity procedures implemented by the agency as a result of the evaluation performed under section

~~3554(a)(1)(F) of title 44, United States Code;~~ ~~and~~

~~(2) the overall cybersecurity posture of the agency, which may include an evaluation of—~~

~~(A) the status of cybersecurity remedial actions of the agency;~~

~~(B) any vulnerability information relating to agency systems that is known to the agency;~~

~~(C) incident information of the agency;~~

~~(D) penetration testing performed by an external entity under section 3559A of title 44, United States Code;~~

~~(E) information from the vulnerability disclosure program information established under section 3559B of title 44, United States Code;~~

~~(F) agency threat hunting results; and~~

~~(G) any other information determined relevant by the Director.~~

~~(c) INDEPENDENT EVALUATION WAIVER.—With respect to an agency that participates in the pilot program under subsection (a) during any year other than the first year during which the pilot program is conducted, the Director, with the concurrence of the Director of the Cybersecurity and Infrastructure Security Agency, may waive any requirement of the agency with respect to the annual~~

independent evaluation under section 3555 of title 44, United States Code.

(f) DURATION.—The pilot program established under this section—

(1) shall be performed over a period of not less than 2 years at each agency that participates in the pilot program under subsection (c), unless the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Council of the Inspectors General on Integrity and Efficiency, determines that continuing the pilot program would reduce the cybersecurity of the agency; and

(2) may be extended by the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Council of the Inspectors General on Integrity and Efficiency, if the Director makes the determination described in paragraph (1).

(g) REPORTS.—

(1) PILOT PROGRAM PLAN.—Before identifying any agencies to participate in the pilot program under subsection (c), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Council of the In-

spectors General on Integrity and Efficiency, shall submit to the appropriate congressional committees a plan for the pilot program that outlines selection criteria and preliminary plans to implement the pilot program.

(2) BRIEFING.—Before commencing a continuous independent evaluation of any agency under the pilot program established under subsection (a), the Director shall provide to the appropriate congressional committees a briefing on—

(A) the selection of agencies to participate in the pilot program; and

(B) processes and procedures to perform a continuous independent evaluation of agencies.

(3) PILOT RESULTS.—Not later than 60 days after the final day of each year during which an agency participates in the pilot program established under subsection (a), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Council of the Inspectors General on Integrity and Efficiency, shall submit to the appropriate congressional committees a report on the results of the pilot program for each agency that participates in the pilot program during that year.

SEC. 302. ACTIVE CYBER DEFENSIVE PILOT.

(a) DEFINITION.—In this section, the term ''active defense technique''—

(1) means an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and

(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques on Federal networks;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A); and

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

(c) PILOT PROGRAM.—Not later than 180 days after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall establish a pilot program at not less than 2 agencies to implement, and assess the effectiveness of, not less than 1 active cyber defense technique.

(d) PURPOSE.—The purpose of the pilot program established under subsection (c) shall be to—

(1) identify any statutory or policy limitations on using active defense techniques;

(2) understand the efficacy of using active defense techniques; and

(3) implement the use of effective techniques to improve agency systems.

(e) PLAN.—Not later than 360 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall develop a plan to offer any active defense technique determined to be successful during the

pilot program established under subsection (c) as a shared service to other agencies.

(f) REPORTS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(1) provide to the appropriate congressional committees a briefing on—

(A) the results of the study performed under subsection (b); and

(B) the agencies selected to participate in the pilot program established under subsection (c);

(2) submit to the appropriate congressional committees a report on the results of the pilot program established under subsection (c), including any recommendations developed from the results of the pilot program; and

(3) submit to the appropriate congressional committees a copy of the plan developed under subsection (c).

(g) SUNSET.—

(1) IN GENERAL.—The requirements of this section shall terminate on the date that is 3 years after the date of enactment of this Act.

(2) AUTHORITY TO CONTINUE USE OF TECHNIQUES.—Notwithstanding paragraph (1), after the date described in paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency may continue to offer any active defense technique determined to be successful during the pilot program established under subsection (c) as a shared service to agencies.

SEC. 303. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

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

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

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

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

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Se-

~~curity and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).~~

~~(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—~~

~~(A) the agreement; and~~

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Federal Information Security Modernization Act of 2021".

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

SEC. 3. DEFINITIONS.

In this Act, unless otherwise specified:

(1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term "additional cybersecurity procedure" has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this Act.

(2) AGENCY.—The term "agency" has the meaning given the term in section 3502 of title 44, United States Code.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

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

(B) the Committee on Oversight and Reform of the House of Representatives; and

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

(4) DIRECTOR.—The term "Director" means the Director of the Office of Management and Budget.

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

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

(7) PENETRATION TEST.—The term "penetration test" has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this Act.

(8) THREAT HUNTING.—The term "threat hunting" means proactively and iteratively searching for

threats to systems that evade detection by automated threat detection systems.

TITLE I—UPDATES TO FISMA

SEC. 101. TITLE 44 AMENDMENTS.

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

(1) in section 3504—

(A) in subsection (a)(1)(B)—

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

"(v) confidentiality, disclosure, and sharing of information;";

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

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

"(vi) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, security of information; and";

(B) in subsection (g), by striking paragraph (1) and inserting the following:

"(1) with respect to information collected or maintained by or for agencies—

"(A) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, disclosure, and sharing of the information; and

"(B) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, develop and oversee policies, principles, standards, and guidelines on security of the information; and"; and

(C) in subsection (h)(1)—

(i) in the matter preceding subparagraph (A)—

(I) by inserting "the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director," before "the Director"; and

(II) by inserting a comma before "and the Administrator"; and

(ii) in subparagraph (A), by inserting "security and" after "information technology";

(2) in section 3505—

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

(i) in subparagraph (B)—

(I) by inserting "the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and" before "the Comptroller General"; and

(II) by striking "and" at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning."; and

(B) by striking the second subsection designated as subsection (c);

(3) in section 3506—

(A) in subsection (b)(1)(C), by inserting ", availability" after "integrity"; and

(B) in subsection (h)(3), by inserting "security," after "efficiency,"; and

(4) in section 3513—

(A) by redesignating subsection (c) as subsection (d); and

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

"(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.".

(b) SUBCHAPTER II DEFINITIONS.—

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

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

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

"(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.";

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

"(7) The term 'high value asset' means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

"(8) The term 'major incident' has the meaning given the term in guidance issued by the Director under section 3598(a).";

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

"(10) The term 'penetration test' means a specialized type of assessment that—

"(A) is conducted on an information system or a component of an information system; and

"(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information system or a component of an information system that could be exploited."; and

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

"(12) The term 'shared service' means a centralized business or mission capability that is provided to multiple organizations within an agency or to multiple agencies.".

(2) CONFORMING AMENDMENTS.—

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

(B) TITLE 10.—

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

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

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended by striking "section 3552(b)(6)" and inserting "section 3552(b)".

(iv) SECTION 2339A.—Section 2339a(e)(5) of title 10, United States Code,

is amended by striking "section 3552(b)(6)" and inserting "section 3552(b)".

(C) HIGH-PERFORMANCE COMPUTING ACT OF 1991.—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking "section 3552(b)(6)(A)(i)" and inserting "section 3552(b)(9)(A)(i)".

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

(E) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking "section 3542(b)(2)" and inserting "section 3552(b)".

(F) IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

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

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking "section 3542(b)(2)" and inserting "section 3552(b)"; and

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking "section 3542(b)(2)" and inserting "section 3552(b)".

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

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

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

(ii) in subsection (f)—

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

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

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

(1) in section 3551—

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

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

"(3) recognize the role of the Cybersecurity and Infrastructure Security Agency as the lead entity for operational cybersecurity coordination across the Federal Government;";

(C) in paragraph (5), as so redesignated, by striking "diagnose and improve" and inserting "integrate, deliver, diagnose, and improve";

(D) in paragraph (6), as so redesignated, by striking "and" at the end;

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

(F) by adding at the end the following:

"(8) recognize that each agency has specific mission requirements and, at times, unique cybersecurity requirements to meet the mission of the agency;

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

"(10) recognize that—

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

"(B) in accounting for the differences described in subparagraph (A) and ensuring overall Federal cybersecurity—

"(i) the Office of Management and Budget is the leader for policy development and oversight of Federal cybersecurity;

"(ii) the Cybersecurity and Infrastructure Security Agency is the leader for implementing operations at agencies; and

"(iii) the National Cyber Director is responsible for developing the overall cybersecurity strategy of the United States and

advising the President on matters relating to cybersecurity.";

(2) in section 3553—

*(A) by striking the section heading and inserting "**Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency**".*

(B) in subsection (a)—

(i) in paragraph (1), by inserting "in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director," before "developing and overseeing";

(ii) in paragraph (5)—

(I) by inserting ", in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director," before "agency compliance"; and

(II) by striking "and" at the end; and

(iii) by adding at the end the following:

"(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology—

"(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

"(B) the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal systems.";

(C) in subsection (b)—

(i) by striking the subsection heading and inserting "CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY";

(ii) in the matter preceding paragraph (1), by striking "The Secretary, in consultation with the Director" and inserting "The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the National Cyber Director";

(iii) in paragraph (2)—

(I) in subparagraph (A), by inserting "and reporting requirements

under subchapter IV of this title" after "section 3556"; and

(II) in subparagraph (D), by striking "the Director or Secretary" and inserting "the Director of the Cybersecurity and Infrastructure Security Agency";

(iv) in paragraph (5), by striking "coordinating" and inserting "leading the coordination of";

(v) in paragraph (8), by striking "the Secretary's discretion" and inserting "the Director of the Cybersecurity and Infrastructure Security Agency's discretion"; and

(vi) in paragraph (9), by striking "as the Director or the Secretary, in consultation with the Director," and inserting "as the Director of the Cybersecurity and Infrastructure Security Agency";

(D) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking "each year" and inserting "each year during which agencies are required to submit reports under section 3554(c)";

(ii) by striking paragraph (1);

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

(iv) in paragraph (3), as so redesignated, by striking "and" at the end;

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

"(4) a summary of each assessment of Federal risk posture performed under subsection (i);"; and

(vi) in paragraph (5), by striking the period at the end and inserting "; and";

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

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

"(i) FEDERAL RISK ASSESSMENTS.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of Federal risk posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of those assessments including—

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

"(2) any vulnerability information relating to the systems of an agency that is known by the agency;

"(3) analysis of incident information under section 3597;

"(4) evaluation of penetration testing performed under section 3559A;

"(5) evaluation of vulnerability disclosure program information under section 3559B;

"(6) evaluation of agency threat hunting results;

"(7) evaluation of Federal and non-Federal threat intelligence;

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

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

"(10) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant."; and

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

(i) by striking "regarding the specific" and inserting "that includes a summary of—

"(1) the specific";

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting "; and" and

(iii) by adding at the end the following:

"(2) the trends identified in the Federal risk assessment performed under subsection (i)."; and

(H) by adding at the end the following:

"(n) BINDING OPERATIONAL DIRECTIVES.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under this section, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate reporting entities the status of the implementation of the binding operational directive at the agency.";

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by redesignating subparagraphs (A), (B), and (C) as subparagraphs (B), (C), and (D), respectively;

(II) by inserting before subparagraph (B), as so redesignated, the following:

"(A) on an ongoing and continuous basis, performing agency system risk assessments that—

"(i) identify and document the high value assets of the agency using guidance from the Director;

"(ii) evaluate the data assets inventoried under section 3511 for sensitivity to compromises in confidentiality, integrity, and availability;

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

"(iv) evaluate the threats facing agency systems and data, including high value assets, based on Federal and non-Federal cyber threat intelligence products, where available;

"(v) evaluate the vulnerability of agency systems and data, including high value assets, including by analyzing—

"(I) the results of penetration testing performed by the Department of Homeland Security under section 3553(b)(9);

"(II) the results of penetration testing performed under section 3559A;

"(III) information provided to the agency through the vulnerability disclosure program of the agency under section 3559B;

"(IV) incidents; and

"(V) any other vulnerability information relating to agency systems that is known to the agency;

"(vi) assess the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (iv) and the agency systems identified under clause (iii); and

"(vii) assess the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or oper-

ational reliance on the operations of the system or data in the system;";

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking "providing information" and inserting "using information from the assessment conducted under subparagraph (A), providing, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, information";

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

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

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

(V) by adding at the end the following:

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

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

"(ii) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

"(I) the Director;

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

"(III) the National Cyber Director;

"(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

"(i) be completed considering the agency system risk assessment performed under subparagraph (A); and

"(ii) include a specific evaluation for high value assets;

"(G) not later than 30 days after completing the evaluation performed under subparagraph (F), providing the evaluation and an implementation plan, if applicable, for using additional cybersecurity procedures determined to be appropriate to—

"(i) the Director of the Cybersecurity and Infrastructure Security Agency;

"(ii) the Director; and

"(iii) the National Cyber Director; and

"(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency in accordance with the risk-based cyber budget model developed pursuant to section 3553(a)(7);";

(ii) in paragraph (2)—

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

(II) in subparagraph (B)—

(aa) by striking "in accordance with standards" and inserting "in accordance with—

"(i) standards"; and

(bb) by adding at the end the following:

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

"(iii) the implementation plan described in paragraph (1)(G);"; and

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

(iii) in paragraph (3)—

(I) in subparagraph (A)—

(aa) in clause (iii), by striking "and" at the end;

(bb) in clause (iv), by adding "and" at the end; and

(cc) by adding at the end the following:

"(v) ensure that—

"(I) senior agency information security officers of component agencies carry out responsibilities under this subchapter, as directed by the senior agency information security officer of the agency or an equivalent official; and

"(II) senior agency information security officers of component agencies report to—

"(aa) the senior information security officer of the agency or an equivalent official; and

"(bb) the Chief Information Officer of the component agency or an equivalent official;"; and

(iv) in paragraph (5), by inserting "and the Director of the Cybersecurity and Infrastructure Security Agency" before "on the effectiveness";

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:

"(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk

assessments, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;";

(ii) in paragraph (2)—

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

"(B) comply with the risk-based cyber budget model developed pursuant to section 3553(a)(7);"; and

(II) in subparagraph (D)—

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

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

"(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3553;"; and

(cc) in clause (iv), as so redesignated, by striking "as determined by the agency; and" and

inserting "as determined by the agency, considering—

"(I) the agency risk assessment performed under subsection (a)(1)(A); and

"(II) the determinations of applying more stringent standards and additional cybersecurity procedures pursuant to section 11331(c)(1) of title 40; and";

(iii) in paragraph (5)(A), by inserting ", including penetration testing, as appropriate," after "shall include testing";

(iv) in paragraph (6), by striking "planning, implementing, evaluating, and documenting" and inserting "planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting";

(v) by redesignating paragraphs (7) and (8) as paragraphs (8) and (9), respectively;

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

"(7) a process for providing the status of every remedial action and known system vulnerability to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;"; and

(vii) in paragraph (8)(C), as so redesignated—

(I) by striking clause (ii) and inserting the following:

"(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3594;";

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

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

"(iii) performing the notifications and other activities required under subchapter IV of this title; and"; and

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

(aa) in subclause (I), by striking "and relevant offices of inspectors general";

(bb) in subclause (II), by adding "and" at the end;

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

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

(ii) by striking paragraph (1) and inserting the following:

"(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representa-

tives, the Committee on Homeland Security of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

"(A) summarizes the agency system risk assessment performed under subsection (a)(1)(A);

"(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment performed under subsection (a)(1)(A);

"(C) summarizes the evaluation and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether those evaluation and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency; and

"(D) summarizes the status of remedial actions identified by inspector general of the agency, the Comptroller General of the United States, and any other source determined appropriate by the head of the agency.

"(2) UNCLASSIFIED REPORTS.—Each report submitted under paragraph (1)—

"(A) shall be, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

"(B) may include a classified annex.

"(3) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified form of the report submitted by the agency under paragraph (2)(A).

"(4) BRIEFINGS.—During each year during which a report is not required to be submitted under paragraph (1), the Director shall provide to the congressional committees described in paragraph (1) a briefing summarizing current agency and Federal risk postures."; and

(iii) in paragraph (5), as so redesignated, by inserting "including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section"; and

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting "and the Director of the Cybersecurity and Infrastructure Security Agency" after "the Director"; and

(4) in section 3555—

*(A) in the section heading, by striking "**ANNUAL INDEPENDENT**" and inserting "**INDEPENDENT**";*

(B) in subsection (a)—

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

(ii) in paragraph (2)(A), by inserting ", including by penetration testing and analyzing the vulnerability disclosure program of the agency" after "information systems"; and

(iii) by adding at the end the following:

"(3) An evaluation under this section may include recommendations for improving the cybersecurity posture of the agency.";

(C) in subsection (b)(1), by striking "annual";

(D) in subsection (e)(1), by inserting "during which a report is required to be submitted under section 3553(c)" after "Each year";

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

"(f) PROTECTION OF INFORMATION.—(1) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers, including the appropriate congressional committees, shall take appropriate steps to ensure the protection of that information, including safeguarding the information from public disclosure.

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

"(3) With respect to information that is not related to national security systems, agencies and evaluators shall make a summary of the information unclassified and publicly available, including information that does not identify—

"(A) specific information system incidents; or

"(B) specific information system vulnerabilities.";

(F) in subsection (g)(2)—

(i) by striking "this subsection shall" and inserting "this subsection—

"(A) shall";

(ii) in subparagraph (A), as so designated, by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(B) identify any entity that performs an independent evaluation under subsection (b)."; and

(G) by striking subsection (j) and inserting the following:

"(j) GUIDANCE.—

"(1) IN GENERAL.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices

"(2) PRIORITIES.—The guidance developed under paragraph (1) shall prioritize the identification of—

"(A) the most common threat patterns experienced by each agency;

"(B) the security controls that address the threat patterns described in subparagraph (A); and

"(C) any other security risks unique to the networks of each agency."; and

(5) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting "within the Cybersecurity and Infrastructure Security Agency" after "incident center"; and

(B) in paragraph (4), by striking "3554(b)" and inserting "3554(a)(1)(A)".

(d) CONFORMING AMENDMENTS.—

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

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

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

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

"3555. Independent evaluation.".

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

(A) in paragraph (1)(B), in the matter preceding clause (i), by striking "annually thereafter" and inserting "thereafter during the years during which a report is required to be sub-

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

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

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

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

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

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

"SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

"§ 3591. Definitions

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

"(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

"(1) APPROPRIATE REPORTING ENTITIES.—The term 'appropriate reporting entities' means—

"(A) the majority and minority leaders of the Senate;

"(B) the Speaker and minority leader of the House of Representatives;

"(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(D) the Committee on Oversight and Reform of the House of Representatives;

"(E) the Committee on Homeland Security of the House of Representatives;

"(F) the appropriate authorization and appropriations committees of Congress;

"(G) the Director;

"(H) the Director of the Cybersecurity and Infrastructure Security Agency;

"(I) the National Cyber Director;

"(J) the Comptroller General of the United States; and

"(K) the inspector general of any impacted agency.

"(2) AWARDEE.—The term 'awardee'—

"(A) means a person, business, or other entity that receives a grant from, or is a party to a cooperative agreement with, an agency; and

"(B) includes any subgrantee of a person, business, or other entity described in subparagraph (A).

"(3) BREACH.—The term 'breach' means—

"(A) a compromise of the security, confidentiality, or integrity of data in electronic form that results in unauthorized access to, or an acquisition of, personal information; or

"(B) a loss of data in electronic form that results in unauthorized access to, or an acquisition of, personal information.

"(4) CONTRACTOR.—The term 'contractor' means—

"(A) a prime contractor of an agency or a subcontractor of a prime contractor of an agency; and

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

"(5) FEDERAL INFORMATION.—The term 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form.

"(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an agency, a contractor, or another organization on behalf of an agency.

"(7) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

"(8) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means a consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

"(9) VULNERABILITY DISCLOSURE.—The term 'vulnerability disclosure' means a vulnerability identified under section 3559B.

"§ 3592. Notification of breach

"(a) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with a senior privacy officer of the agency, shall—

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

"(A) the nature and sensitivity of the personally identifiable information affected by the breach;

"(B) the likelihood of access to and use of the personally identifiable information affected by the breach;

"(C) the type of breach; and

"(D) any other factors determined by the Director; and

"(2) as appropriate, provide written notice in accordance with subsection (b) to each individual potentially affected by the breach—

"(A) to the last known mailing address of the individual; or

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

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

"(1) a brief description of the rationale for the determination that notice should be provided under subsection (a);

"(2) if possible, a description of the types of personally identifiable information affected by the breach;

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

"(A) shall include an e-mail address or another digital contact mechanism; and

"(B) may include a telephone number or a website;

"(4) information on any remedy being offered by the agency;

"(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identi-

fiable information, including relevant information to contact Federal law enforcement agencies and each nationwide consumer reporting agency; and

"(6) any other appropriate information, as determined by the head of the agency or established in guidance by the Director.

"(c) DELAY OF NOTIFICATION.—

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

"(A) impede a criminal investigation or a national security activity;

"(B) reveal sensitive sources and methods;

"(C) cause damage to national security; or

"(D) hamper security remediation actions.

"(2) DOCUMENTATION.—

"(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the Director, the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

"(B) CONTENTS.—A report required under subparagraph (A) shall include a written statement from the entity that delayed the notification explaining the need for the delay.

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

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

"(d) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

"(e) EXEMPTION FROM NOTIFICATION.—

"(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under

subsection (a) if the information affected by the breach is determined by an independent evaluation to be unreadable, including, as appropriate, instances in which the information is—

"(A) encrypted; and

"(B) determined by the Director of the Cybersecurity and Infrastructure Security Agency to be of sufficiently low risk of exposure.

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

"(A) the Director of the Cybersecurity and Infrastructure Security Agency; and

"(B) the Attorney General.

"(3) DOCUMENTATION.—Any exemption granted by the Director under paragraph (1) shall be reported in writing to the head of the agency and the inspector general of the agency that experienced the breach and the Director of the Cybersecurity and Infrastructure Security Agency.

"(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

"(1) the Director from issuing guidance relating to notifications or the head of an agency from noti-

fying individuals potentially affected by breaches that are not determined to be major incidents; or

"(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by breaches.

"§ 3593. Congressional and Executive Branch reports

"(a) INITIAL REPORT.—

"(1) IN GENERAL.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entities a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—

"(A) the information known at the time of the report;

"(B) the sensitivity of the details associated with the major incident; and

"(C) the classification level of the information contained in the report.

"(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent permitted by applicable law, including privacy and statistical laws—

"(A) a summary of the information available about the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

"(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exemption to notification to individuals potentially affected by the major incident under subsection (c) or (e) of section 3592; and

"(C) if applicable, an assessment of the impacts to the agency, the Federal Government, or

the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

"(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 30 days after the date on which an agency submits a written report under subsection (a), the head of the agency shall provide to the appropriate reporting entities written updates on the major incident and, to the extent practicable, provide a briefing to the congressional committees described in subsection (a)(1), including summaries of—

"(1) vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

"(2) any risk assessment and subsequent risk-based security implementation of the affected information system before the date on which the major incident occurred;

"(3) the status of compliance of the affected information system with applicable security requirements at the time of the major incident;

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

"(5) an assessment of the risk of harm to individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

"(6) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident based on information available to agency officials as of the date on which the agency provides the update; and

"(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d) and status updates on the notification process described in section 3592(a), including any delay or exemption described in subsection (c) or (e), respectively, of section 3592, if applicable.

"(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

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

"(e) DELAY AND EXEMPTION REPORT.—

"(1) IN GENERAL.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

"(2) COMPONENT OF OTHER REPORT.—The Director may submit the report required under paragraph (1) as a component of the annual report submitted under section 3597(b).

"(f) REPORT DELIVERY.—Any written report required to be submitted under this section may be submitted in a paper or electronic format.

"(g) THREAT BRIEFING.—

"(1) IN GENERAL.—Not later than 7 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency, jointly with the National Cyber Director and any other Federal entity determined appropriate by the National Cyber Director, shall provide a briefing to the congressional committees described in

subsection (a)(1) on the threat causing the major incident.

"(2) COMPONENTS.—The briefing required under paragraph (1)—

"(A) shall, to the greatest extent practicable, include an unclassified component; and

"(B) may include a classified component.

"(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

"(1) the ability of an agency to provide additional reports or briefings to Congress; or

"(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

"§ 3594. Government information sharing and incident response

"(a) IN GENERAL.—

"(1) INCIDENT REPORTING.—The head of each agency shall provide any information relating to any incident, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget.

"(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall—

"(A) include detailed information about the safeguards that were in place when the incident occurred;

"(B) whether the agency implemented the safeguards described in subparagraph (A) correctly;

"(C) in order to protect against a similar incident, identify—

"(i) how the safeguards described in subparagraph (A) should be implemented differently; and

"(ii) additional necessary safeguards; and

"(D) include information to aid in incident response, such as—

"(i) a description of the affected systems or networks;

"(ii) the estimated dates of when the incident occurred; and

"(iii) information that could reasonably help identify the party that conducted the incident.

"(3) INFORMATION SHARING.—To the greatest extent practicable, the Director of the Cybersecurity and Infrastructure Security Agency shall share information relating to an incident with any agencies that may be impacted by the incident.

"(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

"(b) COMPLIANCE.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director

"(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notifica-

tion granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—

"(1) incident response and recovery; and

"(2) recommendations for mitigating future incidents.

"§ 3595. Responsibilities of contractors and awardees

"(a) NOTIFICATION.—

"(1) IN GENERAL.—Unless otherwise specified in a contract, grant, or cooperative agreement, any contractor or awardee of an agency shall report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency, if the contractor or awardee has a reasonable basis to conclude that—

"(A) an incident or breach has occurred with respect to Federal information collected, used, or maintained by the contractor or awardee in connection with the contract, grant, or cooperative agreement of the contractor or awardee;

"(B) an incident or breach has occurred with respect to a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, or cooperative agreement of the contractor or awardee; or

"(C) the contractor or awardee has received information from the agency that the contractor or awardee is not authorized to receive in connection with the contract, grant, or cooperative agreement of the contractor or awardee.

"(2) PROCEDURES.—

"(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

"(B) INCIDENT.—Following a report of an incident by a contractor or awardee under paragraph (1), an agency, in consultation with the contractor or awardee, shall carry out the requirements under section 3594 with respect to the incident.

"(b) EFFECTIVE DATE.—This section shall apply on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2021.

"§ 3596. Training

"(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to Federal information or Federal information systems because of the status of the individual as an employee, contractor, awardee, volunteer, or intern of an agency.

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

"(1) the internal process of the agency for reporting an incident; and

"(2) the obligation of a covered individual to report to the agency a confirmed major incident and any suspected incident involving information in any medium or form, including paper, oral, and electronic.

"(c) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (b) may be included as part of an annual privacy or security awareness training of an agency.

"§ 3597. Analysis and report on Federal incidents

"(a) ANALYSIS OF FEDERAL INCIDENTS.—

"(1) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop, in consulta-

tion with the Director and the National Cyber Director, and perform continuous monitoring and quantitative and qualitative analyses of incidents at agencies, including major incidents, including—

"(A) the causes of incidents, including—

"(i) attacker tactics, techniques, and procedures; and

"(ii) system vulnerabilities, including zero days, unpatched systems, and information system misconfigurations;

"(B) the scope and scale of incidents at agencies;

"(C) cross Federal Government root causes of incidents at agencies;

"(D) agency incident response, recovery, and remediation actions and the effectiveness of those actions, as applicable; and

"(E) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents.

"(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

"(3) SHARING OF DATA AND ANALYSIS.—

"(A) IN GENERAL.—The Director shall share on an ongoing basis the analyses required under this subsection with agencies and the National Cyber Director to—

"(i) improve the understanding of cybersecurity risk of agencies; and

"(ii) support the cybersecurity improvement efforts of agencies.

"(B) FORMAT.—In carrying out subparagraph (A), the Director shall share the analyses—

"(i) in human-readable written products; and

"(ii) to the greatest extent practicable, in machine-readable formats in order to enable automated intake and use by agencies.

"(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entities a report that includes—

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

"(2) the quantitative and qualitative analyses of incidents developed under subsection (a)(1), including specific analysis of breaches, on an agency-by-agency basis and comprehensively across the Federal Government; and

"(3) an annex for each agency that includes—

"(A) a description of each major incident; and

"(B) the total number of compromises of the agency.

"(c) PUBLICATION.—A version of each report submitted under subsection (b) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

"(d) INFORMATION PROVIDED BY AGENCIES.—

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

"(2) NONCOMPLIANCE REPORTS.—

"(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes—

"(i) data for the incident; and

"(ii) the information described in subsection (b) with respect to the agency.

"(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

"(3) NATIONAL SECURITY SYSTEM REPORTS.—

"(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the agency to the ex-

tent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

"(i) the the majority and minority leaders of the Senate,

"(ii) the Speaker and minority leader of the House of Representatives;

"(iii) the Committee on Homeland Security and Governmental Affairs of the Senate;

"(iv) the Select Committee on Intelligence of the Senate;

"(v) the Committee on Armed Services of the Senate;

"(vi) the Committee on Oversight and Reform of the House of Representatives;

"(vii) the Committee on Homeland Security of the House of Representatives;

"(viii) the Permanent Select Committee on Intelligence of the House of Representatives; and

"(ix) the Committee on Armed Services of the House of Representatives.

"(B) CLASSIFIED FORM.—A report required under subparagraph (A) may be submitted in a classified form.

"(e) REQUIREMENT FOR COMPILING INFORMATION.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

"§ 3598. Major incident definition

"(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

"(b) REQUIREMENTS.—With respect to the guidance issued under subsection (a), the definition of the term 'major incident' shall—

"(1) include, with respect to any information collected or maintained by or on behalf of an agency

or an information system used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency—

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

"(i) the national security, homeland security, or economic security of the United States; or

"(ii) the civil liberties or public health and safety of the people of the United States;

"(B) any incident the head of the agency determines likely to result in an inability for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

"(C) any incident that the head of an agency, in consultation with a senior privacy officer of the agency, determines is likely to have a significant privacy impact on 1 or more individual;

"(D) any incident that the head of the agency, in consultation with a senior privacy official of the agency, determines is likely to have a sub-

stantial privacy impact on a significant number of individuals;

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

"(F) any incident involving the exposure of sensitive agency information to a foreign entity, such as the communications of the head of the agency, the head of a component of the agency, or the direct reports of the head of the agency or the head of a component of the agency; and

"(G) any other type of incident determined appropriate by the Director;

"(2) stipulate that the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident—

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

"(B) is enabled by—

"(i) a common technical root cause, such as a supply chain compromise, a common software or hardware vulnerability; or

"(ii) the related activities of a common threat actor; and

"(3) stipulate that, in determining whether an incident constitutes a major incident because that incident—

"(A) is any incident described in paragraph (1), the head of an agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency;

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

"(C) is an incident described in subparagraph (C) or (D) of paragraph (1), the head of the agency shall consult with—

"(i) the Privacy and Civil Liberties Oversight Board; and

"(ii) the Executive Director of the Federal Trade Commission.

"(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In determining what constitutes a significant number of individuals under subsection (b)(1)(D), the Director—

"(1) may determine a threshold for a minimum number of individuals that constitutes a significant amount; and

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

"(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

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

"(2) the definition of the term 'major incident' included in the guidance issued under subsection (a); and

"(3) an explanation of, and the analysis that led to, the definition described in paragraph (2).".

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

"SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

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

(a) INFORMATION TECHNOLOGY MODERNIZATION CENTERS OF EXCELLENCE PROGRAM ACT.—Section

2(c)(4)(A)(ii) of the Information Technology Modernization Centers of Excellence Program Act (40 U.S.C. 11301 note) is amended by striking the period at the end and inserting ", which shall be provided in coordination with the Director of the Cybersecurity and Infrastructure Security Agency.".

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

(1) in section 1077(b)—

(A) in paragraph (5)(A), by inserting "improving the cybersecurity of systems and" before "cost savings activities"; and

(B) in paragraph (7)—

(i) in the paragraph heading, by striking "CIO" and inserting "CIO";

(ii) by striking "In evaluating projects" and inserting the following:

"(A) CONSIDERATION OF GUIDANCE.—In evaluating projects";

(iii) in subparagraph (A), as so designated, by striking "under section 1094(b)(1)" and inserting "by the Director"; and

(iv) by adding at the end the following:

"(B) CONSULTATION.—In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the necessary stakeholders to ensure the project appropriately addresses cybersecurity risks, including the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate."; and

(2) in section 1078—

(A) by striking subsection (a) and inserting the following:

"(a) DEFINITIONS.—In this section:

"(1) AGENCY.—The term 'agency' has the meaning given the term in section 551 of title 5, United States Code.

"(2) HIGH VALUE ASSET.—The term 'high value asset' has the meaning given the term in section 3552 of title 44, United States Code.";

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

"(8) PROPOSAL EVALUATION.—The Director shall—

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

"(B) require that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a supply chain risk management plan, to be reviewed by the member of the Technology Modernization Board described in subsection (c)(5)(C)."; and

(C) in subsection (c)—

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

(ii) in paragraph (5)—

(I) in subparagraph (A), by striking "and" at the end;

(II) in subparagraph (B), by striking the period at the end and inserting "and"; and

(III) by adding at the end the following:

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

(iii) in paragraph (6)(A), by striking "shall be—" and all that follows through "4

employees'' and inserting ''shall be 4 employees''.

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

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,'';

(B) in subsection (c)—

(i) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking ''including data'' and inserting ''which shall—

''(i) include data'';

(bb) in clause (i), as so designated, by striking '', and performance'' and inserting ''security, and performance; and''; and

(cc) by adding at the end the following:

"(ii) specifically denote cybersecurity funding under the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44."; and

(II) in subparagraph (B), adding at the end the following:

"(iii) The Director shall provide to the National Cyber Director any cybersecurity funding information described in subparagraph (A)(ii) that is provided to the Director under clause (ii) of this subparagraph."; and

(ii) in paragraph (4)(B), in the matter preceding clause (i), by inserting "not later than 30 days after the date on which the review under subparagraph (A) is completed," before "the Administrator";

(C) in subsection (f)—

(i) by striking "heads of executive agencies to develop" and inserting "heads of executive agencies to—

"(1) develop";

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following:

"(2) consult with the Director of the Cybersecurity and Infrastructure Security Agency for the development and use of supply chain security best practices."; and

(D) in subsection (h), by inserting ", including cybersecurity performances," after "the performances"; and

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

(i) in clause (i), by striking "or" at the end;

(ii) in clause (ii), by adding "or" at the end; and

(iii) by adding at the end the following:

"(iii) whether the function should be performed by a shared service offered by another executive agency;"; and

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

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

(1) in section 11312(a), by inserting ", including security risks" after "managing the risks";

(2) in section 11313(1), by striking "efficiency and effectiveness" and inserting "efficiency, security, and effectiveness";

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

"(d) COMPONENT AGENCY CHIEF INFORMATION OFFICERS.—The Chief Information Officer or an equivalent official of a component agency shall report to—

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

"(2) the head of the component agency.";

(4) in section 11317, by inserting "security," before "or schedule"; and

(5) in section 11319(b)(1), in the paragraph heading, by striking "CIOS" and inserting "CHIEF INFORMATION OFFICERS".

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

(1) in subsection (a), by striking "section 3532(b)(1)" and inserting "section 3552(b)";

(2) in subsection (b)(1)(A)—

(A) by striking "in consultation" and inserting "in coordination"; and

(B) by striking "the Secretary of Homeland Security" and inserting "the Director of the Cybersecurity and Infrastructure Security Agency";

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

"(c) APPLICATION OF MORE STRINGENT STANDARDS.—

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

"(A) evaluate, in consultation with the senior agency information security officers, the need to employ standards for cost-effective, risk-based information security for all systems, operations, and assets within or under the supervision of the agency that are more stringent than the standards promulgated by the Director under this section, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

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

"(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

"(A) the status of cybersecurity remedial actions of the agency;

"(B) any vulnerability information relating to agency systems that is known to the agency;

"(C) incident information of the agency;

"(D) information from—

"(i) penetration testing performed under section 3559A of title 44; and

"(ii) information from the vulnerability disclosure program established under section 3559B of title 44;

"(E) agency threat hunting results under section 205 of the Federal Information Security Modernization Act of 2021;

"(F) Federal and non-Federal threat intelligence;

"(G) data on compliance with standards issued under this section;

"(H) agency system risk assessments performed under section 3554(a)(1)(A) of title 44; and

"(I) any other information determined relevant by the head of the agency.";

(4) in subsection (d)(2)—

(A) in the paragraph heading, by striking "NOTICE AND COMMENT" and inserting "CONSULTATION, NOTICE, AND COMMENT";

(B) by inserting "promulgate," before "significantly modify"; and

(C) by striking "shall be made after the public is given an opportunity to comment on the Director's proposed decision." and inserting "shall be made—

"(A) for a decision to significantly modify or not promulgate such a proposed standard, after the public is given an opportunity to comment on the Director's proposed decision;

"(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller

General of the United States, and the Council of the Inspectors General on Integrity and Efficiency;

"(C) considering the Federal risk assessments performed under section 3553(i) of title 44; and

"(D) considering the extent to which the proposed standard reduces risk relative to the cost of implementation of the standard."; and

(5) by adding at the end the following:

"(e) REVIEW OF OFFICE OF MANAGEMENT AND BUDGET GUIDANCE AND POLICY.—

"(1) CONDUCT OF REVIEW.—

"(A) IN GENERAL.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including an assessment of the requirements for agencies to

report information to the Director, and determine whether any changes to that guidance or policy is appropriate.

"(B) FEDERAL RISK ASSESSMENTS.—In conducting the review described in subparagraph (A), the Director shall consider the Federal risk assessments performed under section 3553(i) of title 44.

"(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the results of the review.

"(3) PUBLIC REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall make publicly available a report that includes—

"(A) an overview of the guidance and policy promulgated under this section that is currently in effect;

"(B) the cybersecurity risk mitigation, or other cybersecurity benefit, offered by each guid-

ance or policy document described in subparagraph (A); and

"(C) a summary of the guidance or policy to which changes were determined appropriate during the review and what the changes are anticipated to include.

"(4) CONGRESSIONAL BRIEFING.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the review.

"(f) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the automated verification of the implementation of the controls within the standard.".

SEC. 103. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

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

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

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

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

(ii) the use of automation and machine-readable formats for collecting, compiling, monitoring, and analyzing data; and

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

(2) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall

provide to the appropriate congressional committees a briefing on—

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

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

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

(1) FISMA.—Section 2 of the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554 note) is amended—

(A) by striking subsection (b); and

(B) by redesignating subsections (c) through (f) as subsections (b) through (e), respectively.

(2) INCIDENT DATA SHARING.—

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

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

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

(I) the causes of incidents;

(II) the scope and scale of incidents within the environments and systems of an agency;

(III) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(IV) agency response, recovery, and remediation actions and the effectiveness of those actions; and

(V) the impact of incidents;

(ii) enable the efficient development of—

(I) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

(II) the report on Federal incidents required under section 3597(b) of

title 44, United States Code, as added by this Act;

(iii) include requirements for the timeliness of data production; and

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

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 3594(c) of title 44, United States Code, as added by this Act, to provide information to other agencies experiencing incidents.

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this Act.

(5) CONTRACTOR AND AWARDEE GUIDANCE.—

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

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

(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).

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

(1) in paragraph (11), by striking "or" at the end;

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

(3) by adding at the end the following:

"(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.".

SEC. 104. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

(1) performing the ongoing and continuous agency system risk assessment required under section

3554(a)(1)(A) of title 44, United States Code, as amended by this Act;

(2) implementing additional cybersecurity procedures, which shall include resources for shared services;

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44, United States Code, as amended by this Act, to the Director and the Cybersecurity and Infrastructure Security Agency using automation and machine-readable data, as practicable, which shall include—

(A) specific guidance for the use of automation and machine-readable data; and

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

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

(5) a requirement to coordinate with inspectors general of agencies to ensure consistent understanding and application of agency policies for the purpose of evaluations by inspectors general.

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

(a) DEFINITIONS.—In this section:

(1) REPORTING ENTITY.—The term "reporting entity" means private organization or governmental unit that is required by statute or regulation to submit sensitive information to an agency.

(2) SENSITIVE INFORMATION.—The term "sensitive information" has the meaning given the term by the Director in guidance issued under subsection (b).

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

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

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

TITLE II—IMPROVING FEDERAL CYBERSECURITY

SEC. 201. MOBILE SECURITY STANDARDS.

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

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

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

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

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

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

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and Infra-

structure Security Agency, shall issue guidance to agencies for sharing the inventory of the agency required under subsection (b)(1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

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

SEC. 202. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

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

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

(1) the types of logs to be maintained;

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

(3) the time periods for agencies to enable recommended logging and security requirements;

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

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

(A) the Director of the Cybersecurity and Infrastructure Security Agency for a cybersecurity purpose; and

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

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

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney

General, shall, as determined to be appropriate by the Director, update guidance to agencies regarding requirements for logging, log retention, log management, sharing of log data with other appropriate agencies, or any other logging activity determined to be appropriate by the Director.

SEC. 203. CISA AGENCY ADVISORS.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 1 cybersecurity professional employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the senior agency information security officer of each agency.

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

(1) cybersecurity threats facing agencies, including any specific threats to the assigned agency;

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

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

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

(2) serving as an incident response point of contact between the assigned agency and the Cybersecurity and Infrastructure Security Agency; and

(3) familiarizing themselves with agency systems, processes, and procedures to better facilitate support to the agency in responding to incidents.

(d) LIMITATION.—An advisor assigned under subsection (a) shall not be a contractor.

(e) MULTIPLE ASSIGNMENTS.—One individual advisor may be assigned to multiple agency Chief Information Officers under subsection (a).

SEC. 204. FEDERAL PENETRATION TESTING POLICY.

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

"§ 3559A. Federal penetration testing

"(a) DEFINITIONS.—In this section:

"(1) AGENCY OPERATIONAL PLAN.—The term 'agency operational plan' means a plan of an agency for the use of penetration testing.

"(2) RULES OF ENGAGEMENT.—The term 'rules of engagement' means a set of rules established by an agency for the use of penetration testing.

"(b) GUIDANCE.—

"(1) IN GENERAL.—The Director shall issue guidance that—

"(A) requires agencies to use, when and where appropriate, penetration testing on agency systems; and

"(B) requires agencies to develop an agency operational plan and rules of engagement that meet the requirements under subsection (c).

"(2) PENETRATION TESTING GUIDANCE.—The guidance issued under this section shall—

"(A) permit an agency to use, for the purpose of performing penetration testing—

"(i) a shared service of the agency or another agency; or

"(ii) an external entity, such as a vendor; and

"(B) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, without regard to the status of the entity that performs the penetration testing.

"(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

"(1) require the agency to—

"(A) perform penetration testing on the high value assets of the agency; or

"(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed;

"(2) establish guidelines for avoiding, as a result of penetration testing—

"(A) adverse impacts to the operations of the agency;

"(B) adverse impacts to operational environments and systems of the agency; and

"(C) inappropriate access to data;

"(3) require the results of penetration testing to include feedback to improve the cybersecurity of the agency; and

"(4) include mechanisms for providing consistently formatted, and, if applicable, automated and machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

"(d) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

"(1) establish a process to assess the performance of penetration testing by both Federal and non-Federal entities that establishes minimum quality controls for penetration testing;

"(2) develop operational guidance for instituting penetration testing programs at agencies;

"(3) develop and maintain a centralized capability to offer penetration testing as a service to Federal and non-Federal entities; and

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

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

"(1) not less frequently than annually, inventory all Federal penetration testing assets; and

"(2) develop and maintain a standardized process for the use of penetration testing.

"(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.—

"(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop a framework for prioritizing Federal penetration testing resources among agencies.

"(2) CONSIDERATIONS.—In developing the framework under this subsection, the Director shall consider—

"(A) agency system risk assessments performed under section 3554(a)(1)(A);

"(B) the Federal risk assessment performed under section 3553(i);

"(C) the analysis of Federal incident data performed under section 3597; and

"(D) any other information determined appropriate by the Director or the Director of the Cybersecurity and Infrastructure Security Agency.

"(g) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The guidance issued under subsection (b) shall not apply to national security systems.

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

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

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

(b) DEADLINE FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director

shall issue the guidance required under section 3559A(b) of title 44, United States Code, as added by subsection (a).

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

"3559A. Federal penetration testing.".

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

(1) in paragraph (8)(B), by striking "and" at the end;

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

(3) by inserting after paragraph (8) the following:

"(9) performing penetration testing with or without advance notice to, or authorization from, agencies, to identify vulnerabilities within Federal information systems; and".

SEC. 205. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

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

esis-driven threat-hunting services on the network of each agency.

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish the program required under paragraph (1) that describes how the Director of the Cybersecurity and Infrastructure Security Agency plans to—

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

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

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

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

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

(ii) additional cybersecurity procedures under section 3554 of title 44, United States Code.

(b) REPORTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(1) not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security Agency completes the plan required under subsection (a)(2), a report on the plan to provide threat hunting services to agencies;

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program under subsection (a)(1), a report providing any updates to the plan developed under subsection (a)(2); and

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services to agencies other than the Cybersecurity and Infrastructure Security Agency, a report describing lessons learned from providing those services.

SEC. 206. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section 204 of this Act, the following:

"§ 3559B. Federal vulnerability disclosure programs

"(a) DEFINITIONS.—In this section:

"(1) REPORT.—The term 'report' means a vulnerability disclosure made to an agency by a reporter.

"(2) REPORTER.—The term 'reporter' means an individual that submits a vulnerability report pursuant to the vulnerability disclosure process of an agency.

"(b) RESPONSIBILITIES OF OMB.—

"(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that conducts a security research activity that the head of the agency determines—

"(A) represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (d)(2); and

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

"(2) SHARING INFORMATION WITH CISA.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a con-

sistent, automated, and machine readable manner with the Cybersecurity and Infrastructure Security Agency, including—

"(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on Federal information systems that use commercial software or services;

"(B) information relating to vulnerability disclosure, coordination, or remediation activities of an agency, particularly as those activities relate to outside organizations—

"(i) with which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency can assist; or

"(ii) about which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency should know; and

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

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

"(c) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

"(1) provide support to agencies with respect to the implementation of the requirements of this section;

"(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section; and

"(3) upon a request by an agency, assist the agency in the disclosure to vendors of newly identified vulnerabilities in vendor products and services.

"(d) RESPONSIBILITIES OF AGENCIES.—

"(1) PUBLIC INFORMATION.—The head of each agency shall make publicly available, with respect to each internet domain under the control of the agency that is not a national security system—

"(A) an appropriate security contact; and

"(B) the component of the agency that is responsible for the internet accessible services offered at the domain.

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

"(A) describe—

"(i) the scope of the systems of the agency included in the vulnerability disclosure policy;

"(ii) the type of information system testing that is authorized by the agency;

"(iii) the type of information system testing that is not authorized by the agency; and

"(iv) the disclosure policy of the agency for sensitive information;

"(B) with respect to a report to an agency, describe—

"(i) how the reporter should submit the report; and

"(ii) if the report is not anonymous, when the reporter should anticipate an acknowledgment of receipt of the report by the agency;

"(C) include any other relevant information; and

"(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

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

"(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program established under this section.

"(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.

"(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infra-

structure Security Agency under this section shall not apply to national security systems.

"(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director and the Director of the Cybersecurity and Infrastructure Security Agency described in this section shall be delegated—

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

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

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

"3559B. Federal vulnerability disclosure programs.".

SEC. 207. IMPLEMENTING PRESUMPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

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

(1) shifting away from "trusted networks" to implement security controls based on a presumption of compromise;

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

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

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

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

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

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

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director;

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

(3) a schedule to implement any planned activities.

SEC. 208. AUTOMATION REPORTS.

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

(b) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes by agencies.

SEC. 209. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

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

SEC. 210. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

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

(1) in subparagraph (A), by striking "and" at the end;

(2) by redesignating subparagraph (B) as subparagraph (C); and

(3) by inserting after subparagraph (A) the following:

"(B) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44, United States Code; and".

TITLE III—RISK-BASED BUDGET MODEL

SEC. 301. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

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

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

(2) COVERED AGENCY.—The term "covered agency" has the meaning given the term "executive agency" in section 133 of title 41, United States Code.

(3) DIRECTOR.—The term "Director" means the Director of the Office of Management and Budget.

(4) INFORMATION TECHNOLOGY.—The term "information technology"—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

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

(5) RISK-BASED BUDGET.—The term "risk-based budget" means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

SEC. 302. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) IN GENERAL.—

(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Director of the National Institute of Standards and Technology, shall develop a standard model for creating a risk-based budget for cybersecurity spending.

(2) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section 101, is further amended by inserting after paragraph (6) the following:

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

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—

(A) consider Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(B) consider the impact of agency operations of compromise of systems, including the interconnectivity to other agency systems and the operations of other agencies;

(C) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;

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

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

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

(E) be used to evaluate and inform Government-wide cybersecurity programs of the Department of Homeland Security.

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

(5) PUBLICATION.—The Director shall publish the model required to be developed under this subsection, and any updates necessary under paragraph (4), on the public website of the Office of Management and Budget.

(6) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under this subsection is completed, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

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

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

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

(c) VERIFICATION.—

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

(A) in the matter preceding subclause (I), by striking "by agency, and by initiative area (as determined by the administration)" and inserting "and by agency";

(B) in subclause (III), by striking "and" at the end; and

(C) by adding at the end the following:

"(V) a validation that the budgets submitted were developed using a risk-based methodology; and

"(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.".

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) REPORTS.—

(1) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

(A) in subparagraph (B), by striking "and" at the end;

(B) in subparagraph (C), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following:

"(D) an assessment of how the agency implemented the risk-based budget model required under section 3553(a)(7) and an evaluation of whether the model mitigates agency cyber vulnerabilities.".

(2) ASSESSMENT.—Section 3553(c) of title 44, United States Code, as amended by section 101, is further amended by inserting after paragraph (5) the following:

"(6) an assessment of—

"(A) Federal agency implementation of the model required under subsection (a)(7);

"(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

"(C) whether the model mitigates the cyber vulnerabilities of the Federal Government.".

(e) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by subsection (c), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

(2) an evaluation of the success of covered agencies in implementing risk-based budgets;

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerability, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

(4) any other information relating to risk-based budgets the Comptroller General determines appropriate.

TITLE IV—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 401. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term "active defense technique"—

(1) means an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and

(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

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

SEC. 402. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

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

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

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

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

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Com-

mittee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

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

Calendar No. 673

117TH CONGRESS
2D SESSION

S. 2902

[Report No. 117–274]

A BILL

To modernize Federal information security management, and for other purposes.

DECEMBER 19, 2022

Reported with an amendment