[DISCUSSION DRAFT]

117TH CONGRESS
2D SESSION

H. R. _____

To modernize Federal information security management and improve Federal cybersecurity to combat persisting and emerging threats, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M__. _____ introduced the following bill; which was referred to the Committee on _____

A BILL

To modernize Federal information security management and improve Federal cybersecurity to combat persisting and emerging threats, 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 2022''.

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

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

''(v) confidentiality, privacy, disclosure, and sharing of information;'';

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

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

''(vi) in consultation with the National Cyber Director, security of information; and'';

(2) in section 3505—

(A) in paragraph (2) of the first subsection designated as subsection (c) by adding ''discovery of internet-accessible information systems and assets, as well as'' after ''an inventory under this subsection shall include'';

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

(i) in subparagraph (B)—

(I) by inserting ''the Secretary of Homeland Security acting through 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 wherever practicable.''; and

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

(3) in section 3506—

(A) in subsection (a)(3), by inserting ''In carrying out these duties, the Chief Information Officer shall coordinate, as appropriate, with

the Chief Data Officer in accordance with the designated functions under section 3520(c).'' after ''reduction of information collection burdens on the public.'';

(B) in subsection (b)(1)(C), by inserting '', availability'' after ''integrity'';

(C) in subsection (g)—

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

(ii) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(D) 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 to the National Cyber Director.''.

(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), (4), (5), (6), (7), (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 (2), as so redesignated, the following:

''(3) The term 'high value asset' means information or an information system that the head of an agency determines, using policies, principles, standards, or guidelines issued by the Director under section 3553(a), to be 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.'';

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

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

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

''(10) The term 'penetration test' has the meaning given the term in guidance issued by the Director.''; and

(F) 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 Im-

provement 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) in paragraph (4), by striking ''diagnose and improve'' and inserting ''integrate, deliver, diagnose, and improve'';

(B) in paragraph (5), by striking ''and'' at the end;

(C) in paragraph (6), by striking the period at the end and inserting a semicolon; and

(D) by adding at the end the following:

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

''(8) 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

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

(2) in section 3553—

(A) in subsection (a)—

(i) in paragraph (5), by striking ''and'' at the end;

(ii) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(7) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, 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 zero trust architecture principles to improve resiliency and timely response actions to incidents on Federal systems.'';

(B) in subsection (b)—

(i) in the matter preceding paragraph (1), by striking ''The Secretary, in consultation with the Director'' and inserting ''The Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency

and in consultation with the Director and the National Cyber Director'';

(ii) in paragraph (2)(A), by inserting ''and reporting requirements under subchapter IV of this chapter'' after ''section 3556'';

(iii) redesignate paragraphs (8) and (9) as paragraphs (9) and (10); and

(iv) insert a new paragraph (8):

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

''(A) central shared services contracts for cybersecurity capabilities identified as optimal by the Director, in coordination with the Secretary acting through the Director of the Cybersecurity and Infrastructure Security Agency and other agencies as appropriate; and

''(B) offering technical assistance and expertise to agencies on the selection and successful engagement of highly adaptive cybersecurity service contracts and other relevant contracts provided by the U.S. General Services Administration.'';

(C) 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)'' and by striking ''preceding year'' and inserting ''preceding two years'';

(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; and

(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'';

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

(E) in subsection (h)—

(i) in paragraph (2), subparagraph (A) adding ''and the National Cyber Director'' after ''in coordination with the Director'';

(ii) in paragraph (2), subparagraph (D) adding ", the National Cyber Director," after "notify the Director"; and

(iii) in paragraph (3), subparagraph (A), clause (iv) adding ", the National Cyber Director," after "the Secretary provides prior notice to the Director";

(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 cyber 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.'';

(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 assessments 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 7 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 Director and National Cyber Director 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 operational reliance on the operations of the system or data in the system;";

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking "providing information" and inserting "using infor-

mation from the assessment conducted under subparagraph (A), providing information'';

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

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

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

(V) by adding at the end the following:

''(E) providing an update on the ongoing and continuous assessment 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 every 2 years, 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;'';

(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"; and

(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)(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 In-

frastructure Security Agency under section 3553;''; and

(III) in clause (iv), as so redesignated, by striking ''as determined by the agency; and'' and inserting ''as determined by the agency, considering the agency risk assessment performed under subsection (a)(1)(A).'';

(iii) in paragraph (5)(A), by inserting '', including penetration testing, as appropriate,'' after ''shall include testing'';

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

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

''(7) a process for providing the status of every remedial action, as well as unremediated identified system vulnerabilities, 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

(vi) 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 chapter; 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 the enactment of the Federal Information Security Modernization Act of 2022 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 majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, 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 Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology 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), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

"(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,'' after ''policies, procedures, and practices''; 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, 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) striking subsection (j); and

(5) in section 3556(a)(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 submitted 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 or an other transaction 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' shall be defined by the Director.

''(4) CONTRACTOR.—The term 'contractor' means a prime contractor of an agency or a subcontractor of a prime contractor 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 infor-

mation 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 the chief 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 breach;

''(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, mailing address, 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 identifiable information, including relevant contact information for 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 National Cyber Director, 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 potentially affected 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) 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 notifying 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. Within 7 days of a major incident determination, the head of the agency impacted shall coordinate with the National Cyber Director, or their designee, to provide a briefing, along with any other Federal entity determined appropriate by the National Cyber Director, 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, in the manner requested by the Congressional entities, taking into account—

"(A) the information known at the time of the report, including the threat having likely caused the major incident;

"(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 and, if applicable, 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 notification to individuals potentially affected by the major incident under subsection (c) 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.

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

''(A) shall, to the greatest extent practicable, include an unclassified component; and

''(B) may include a classified component.

''(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) 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;

''(4) 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;

''(5) 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

''(6) 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 described in subsection (c) of section 3592, if applicable.

''(c) UPDATE REPORT.—If the agency, or the National Cyber Director, 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 annual report is submitted.

''(e) DELAY REPORT.—

''(1) IN GENERAL.—The Director shall submit to the appropriate reporting entities an annual report on all notification delays granted pursuant to subsection (c) 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) 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.—Subject to limitations in subsection (b), the head of each agency shall provide any information relating to any incident affecting their agency, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency, the Office of Management and Budget, and the Office of the National Cyber Director.

''(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, as appropriate.

''(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, or are potentially susceptible or similarly targeted.

''(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems 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 notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency to facilitate asset response activities and recommendations for mitigating future incidents, and with the Federal Bureau of Investigation to facilitate threat response activities, consistent with relevant policies, principles, standards, and guidelines on information security.

''§ 3595. Responsibilities of contractors and awardees

''(a) REPORTING.—

''(1) IN GENERAL.—Unless otherwise specified in a contract, grant, cooperative agreement, or any other transaction 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 suspect or 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, cooperative agreement, or other transaction 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, cooperative agreement, or other transaction 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, cooperative agreement, or other transaction 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 the enactment of the Federal Information Security Modernization Act of 2022 and shall apply with respect to any contract entered into on or after such effective date.

"§ 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 consultation 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 day exploitations, unpatched systems, and information system misconfigurations;

"(B) the scope and scale of incidents at agencies;

"(C) common root causes of incidents across multiple agencies;

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

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

"(F) trends across multiple Federal agencies to address intrusion detection and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

"(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 the 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, the National Cyber Director, and the heads of other agencies as appropriate, shall submit to the appropriate reporting 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) on an agency-by-agency basis and comprehensively across the Federal Government, including—

"(A) a specific analysis of breaches; and

"(B) an analysis of the Federal Government's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)); and

"(3) an annex for each agency that includes—

"(A) a description of each major incident; and

"(B) an analysis of the agency's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

"(c) PUBLICATION.—To the extent that publication is consistent with national security interests, 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) 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 extent 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 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 Appropriations of the Senate;

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

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

"(ix) the Permanent Select Committee on Intelligence of the House of Representatives;

"(x) the Committee on Armed Services of the House of Representatives; and

"(xi) the Committee on Appropriations 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, the National

Cyber Director, and in consultation with the impacted agency.

"§ 3598. Major incident definition

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of the Federal Information Security Modernization Act of 2022, 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 result in demonstrable harm to—

''(i) the national security interests, foreign relations or the economy of the United States; or

"(ii) the public confidence, civil liberties, or public health and safety of the people of the United States;

"(B) any incident the head of the agency determines may have a significant impact on the confidentiality, integrity, or availability of a high value asset; and

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

"(2) stipulate that the Director, in coordination with the National Cyber Director, shall declare a major incident at each agency impacted by an incident if it is determined 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 or a common software or hardware vulnerability; or

"(ii) the related activities of a common threat actor.

"(c) EVALUATION AND UPDATES.—Not later than 2 years after the date of the enactment of the Federal Information Security Modernization Act of 2022, 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) MODERNIZING GOVERNMENT TECHNOLOGY.—Subtitle G of title X of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115–91; 40 U.S.C. 11301 note) is amended in section 1078—

(1) 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.''; and

(2) in subsection (c)—

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

(B) in paragraph (5)—

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

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

(iii) by adding at the end the following:

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

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

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

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,'';

(B) in subsection (c)(3)(B), by adding at the end the following:

''(iii) The Director may make available, upon request, 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.'';

(C) in subsection (f), by striking ''The Director shall'' and inserting ''The Director shall—

''(1) encourage the heads of the executive agencies to develop and use the best practices in the ac-

quisition of information technology, including supply chain security best practices; and

''(2) consult with the Federal Chief Information Security Officer appointed by the President under section 3607 of title 44, United States Code, 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), in paragraph (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.''.

(c) SUBCHAPTER II.—Subchapter II of chapter 113 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''.

(d) 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), by striking ''the Secretary of Homeland Security'' and inserting ''the

Director of the Cybersecurity and Infrastructure Security Agency'';

(3) 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, as available, 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 Fed-

eral risk assessments performed under section 3553(i) of title 44.

''(C) REQUIREMENTS BURDEN REDUCTION AND CLARITY.—In conducting the review described in subparagraph (A), the Director shall consider the cumulative reporting and compliance burden to agencies as well as the clarity of the requirements and deadlines contained in guidance and policy documents.

''(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) CONGRESSIONAL BRIEFING.—Not later than 60 days after the date on which a review is completed under paragraph (1), the Director is expected to 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 and any newly issued guidance or policy, which shall include—

''(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 guidance 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 include.

''(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 the 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 the 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) 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.

(2) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of the 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.

(3) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of the enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and tem-

plates, 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.

(4) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of the 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.

(5) 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 the enactment of this Act, the Director 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 Director of 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 the 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 the 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 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. 202. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) RECOMMENDATIONS.—Not later than 2 years after the date of the 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 duration that logs and other relevant data should be retained;

(3) the time periods for agency implementation of 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 Director of 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.

(d) SUNSET.—This section will cease to be in effect on the date that is 10 years after the date of enactment of this Act.

SEC. 203. 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) GUIDANCE.—

"(1) IN GENERAL.—The Director shall, in consultation with the Secretary of the Department of

Homeland Security, issue guidance to agencies that—

"(A) requires agencies to use, when and where appropriate, penetration testing on agency systems by both Federal and non-Federal entities, with a focus on high value assets;

"(B) provides policies governing agency development of an operational plan, rules of engagement for utilizing penetration testing, and procedures to utilize the results of penetration testing to improve the cybersecurity and risk management of the agency; and

"(C) establishes a program under the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed appropriately by agencies and to provide operational support or a shared service.

"(b) 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.

''(c) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The guidance issued under subsection (a) shall not apply to national security systems.

''(d) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (a) 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 the enactment of this Act, the Director shall issue the guidance required under section 3559A(a) of title 44, United States Code, as added by subsection (a).

(c) SUNSET.—This section shall sunset on the date that is 10 years after the date of enactment of this Act.

(d) 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.''.

(e) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by section 5121, 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 to identify vulnerabilities within Federal information systems; and''.

SEC. 204. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall, in accordance with the authorities granted the Secretary under sectyions 3553(b)(7)-(8) and 3553(m) of title 44, United States Code (as redesignated by this Act), 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 the 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, analyzing, and safeguarding 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, in consultation with the Director, 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 re-

quired 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. 205. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Subchapter II of Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section 204, 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 of the Office of Management and Budget, 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 of the Office of Management and Budget, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine

readable manner with the Director of 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 Director of 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, covering all internet accessible 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.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of the enactment of the Federal Information Security Modernization Act of 2022, and annually thereafter for a 3-year period, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with 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) SUNSET.—This section shall sunset on the date that is 10 years after the date of enactment of this Act.

(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 3559A, as added by this Act, the following:

''3559B. Federal vulnerability disclosure programs''.

SEC. 206. IMPLEMENTING ZERO TRUST PRINCIPLES.

(a) GUIDANCE.—The Director shall maintain guidance on, and not later than 2 years after the date of the enactment of this Act, provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems through the adoption of zero trust cybersecurity principles across the government, 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 270 days after the date of the 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 a zero trust cybersecurity strategy, which shall include—

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

(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. 207. GAO AUTOMATION REPORT.

Not later than 2 years after the date of the 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 employed by agencies under paragraphs (1), (5)(C), and (8)(B) of section 3554(b) of title 44, United States Code.

SEC. 208. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

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

(b) DESIGNATION.—Section 1322(c)(1) of title 41, United States Code, is amended by striking ''Not later than'' and all that follows through the end of the paragraph and inserting '' The Director of OMB shall designate the Federal Chief Information Security Officer appointed by the President under section 3607 of title 44,

United States Code, or an equivalent senior-level official from the Office of Management and Budget if the position is vacant, to serve as the Chairperson of the Council.''.

(c) DEFINITION.—Section 1321 of title 41, United States Code, is amended by adding the following definition and renumbering accordingly:

''(8) SOFTWARE BILL OF MATERIALS.—The term 'software bill of materials' shall have the meaning given to it by the Administrator of the National Telecommunications and Information Administration.''.

(d) REQUIREMENT.—Subsection 1326(b) of title 41, United States Code, is amended by inserting the following paragraph before paragraph (6) and renumbering all subsequent paragraphs accordingly:

''(6) maintaining an inventory of all available Software Bills of Materials for each software products in use by the agency, as appropriate, to be available to the Federal Acquisition Security Council, the Secretary of Homeland Security acting through the Director of Cybersecurity and Infrastructure Security, and the National Cyber Director.''.

SEC. 209. FEDERAL CHIEF INFORMATION SECURITY OFFICER.

(a) IN GENERAL.—Chapter 36 of title 44, United States Code, is amended by inserting at the end:

"§ 3607. Federal chief information security officer

''(a) ESTABLISHMENT.—There is established in the Office of the Federal Chief Information Officer of the Office of Management and Budget a Federal Chief Information Security Officer, who shall be appointed by the President.

''(b) DUTIES.—The Federal Chief Information Security Officer shall report to the Federal Chief Information Officer, and assist the Chief Information Officer in carrying out—

''(1) all functions under this chapter;

''(2) all functions assigned to the Director under title II of the E-Government Act of 2002;

''(3) other electronic government initiatives, consistent with other statutes; and

''(4) other initiatives determined by the Chief Information Officer.

''(c) ADDITIONAL DUTIES.—The Federal Chief Information Security Officer shall work with the Chief Information Officer to oversee implementation of electronic Government under the E-Government Act of 2002, and other

relevant statutes, in a manner consistent with law, relating to—

''(1) cybersecurity strategy, policy, and operations;

''(2) the development of enterprise architectures;

''(3) information security;

''(4) privacy;

''(5) access to, dissemination of, and preservation of Government information; and

''(6) other areas of electronic Government as determined by the Administrator.

''(d) ASSISTANCE.—The Federal Chief Information Security Officer shall assist the Administrator in the performance of electronic Government functions as described in section 3602(f).''.

(b) IN GENERAL.—Section 1500 of title 6, United States Code, is amended by adding:

''(d) DEPUTY DIRECTOR.—There shall be a Deputy National Cyber Director for Agency Strategy, Capabilities, and Budget, who shall be the Federal Chief Information Security Officer appointed by the President under section 3607 of title 44, United States Code, and shall report to the Director and assist the office in carrying out the fol-

lowing duties as it applies to the protection of Federal information systems by the agencies—

''(1) the preparation and oversight over the implementation of the national cyber policy under subsection (c)(1)(C)(i);

''(2) the formation and issuance of recommendations to agencies on resource allocations and policies under subsection (c)(1)(C)(ii);

''(3) reviewing annual budget proposals and making related recommendations under subsection (c)(1)(C)(iii); and

''(4) other initiatives determined by the Director, or to be necessary to coordinate with the Office by the Federal Chief Information Officer.''.

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

''3607. Federal chief information security officer''.

SEC. 210. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

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''.

SEC. 211. QUANTITATIVE CYBERSECURITY METRICS.

(a) DEFINITION OF COVERED METRICS.—In this section, the term ''covered metrics'' means the metrics established, reviewed, and updated under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(b) UPDATING AND ESTABLISHING METRICS.—Not later than 1 year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—

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

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

(A) update the covered metrics; and

(B) establish new covered metrics.

(c) IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 540 days after the date of the enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promulgate guidance that requires each agency to use covered metrics to track trends in the cybersecurity and incident response capabilities of the agency.

(2) PERFORMANCE DEMONSTRATION.—The guidance issued under paragraph (1) and any subsequent guidance shall require agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency using the covered metrics included in the guidance.

(3) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar penetration tests, as determined by the Director, in coordination with the Director of the Cybersecurity

and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

(4) ANALYSIS CAPACITY.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop a capability that allows for the analysis of the covered metrics, including cross-agency performance of agency cybersecurity and incident response capability trends.

(d) CONGRESSIONAL REPORTS.—

(1) UTILITY OF METRICS.—Not later than 1 year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

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

(e) CYBERSECURITY ACT OF 2015 UPDATES.—Section 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522) is amended—

(1) by amending subsection (c) to read as follows:

''(c) IMPROVED METRICS.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with the responsibilities of agencies under section 3554 of title 44, United States Code.'';

(2) by striking subsection (e); and

(3) by redesignating subsection (f) as subsection (e).

TITLE III—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 301. RISK-BASED BUDGET PILOT.

(a) DEFINITIONS.—In this section:

(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, the Committee on Oversight and Reform, and

the Committee on Appropriations of the House of Representatives.

(2) 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.

(3) 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 cyber 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).

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

(1) IN GENERAL.—

(A) 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 the 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 conduct a pilot for creating a risk-based budget for cybersecurity spending.

(B) CONTENTS OF PILOT.—The pilot required to be developed under paragraph (1) shall—

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

(ii) consider the impact of agency operations of compromise of systems, including the interconnectivity to other agency systems and the operations of other agencies;

(iii) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;

(iv) 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

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

(2) REPORTS.—Not later than 2 years after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of the enactment of this Act, the Director shall submit a report to Congress on the implementation of the pilot for risk-

based budgeting for cybersecurity spending, an assessment of agency implementation, and an evaluation of whether the risk-based budget helps to mitigate cybersecurity vulnerabilities.

(3) 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—

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

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

(C) any other information relating to risk-based budgets the Comptroller General determines appropriate.

SEC. 302. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ''active defense technique'' has the meaning given in guidance

issued by the Director, in coordination with the Attorney General.

(b) STUDY.—Not later than 180 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director and the National Cyber 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 Attorney General;

(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 agency operations and mission delivery, threat re-

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

(a) PURPOSE.—The purpose of this section is for the Director of the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of the head 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 the 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 of the Office of Management and Budget, 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 the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to appropriate congressional committees 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 appropriate congressional committees a report on—

(A) the agreement; and

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

SEC. 304. ENDPOINT DETECTION AND RESPONSE AS A SHARED SERVICE PILOT.

(a) PURPOSE.—The Cybersecurity and Infrastructure Security Agency is directed to establish and conduct a pilot to determine the feasibility, value, and efficacy of providing endpoint detection and response capabilities as a shared service to Federal agencies to reduce costs, enhance interoperability, and continuously detect and mitigate threat activity on Federal networks.

(b) PLAN.—Not later than 60 days 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 endpoint detection and response

shared service offering within the Cybersecurity and Infrastructure Security Agency.

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

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

(2) maximizing the value of existing agency investments in endpoint detection and response tools and services;

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

(4) equipping all endpoints and services of pilot agencies with endpoint detection and response programs;

(5) aggregating endpoint data from both within the agency and across agencies to provide enterprise-wide monitoring of network to detect abnormal network behavior; and

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

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 60 days after the date on which the plan required under subsection (b) is developed, the Director of the Cyberse-

curity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer endpoint detection and response 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 180 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 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).