IB

Union Calendar No. 790

118TH CONGRESS
2D SESSION

H. R. 4552

[Report No. 118–939, Part I]

To improve the cybersecurity of the Federal Government, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 11, 2023

Ms. MACE (for herself, Mr. RASKIN, Mr. COMER, and Mr. CONNOLLY) introduced the following bill; which was referred to the Committee on Oversight and Accountability, and in addition to the Committees on Science, Space, and Technology, Homeland Security, and Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

DECEMBER 19, 2024

Additional sponsor: Mr. DAVIS of North Carolina

DECEMBER 19, 2024

Reported from the Committee on Oversight and Accountability with an amendment

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

DECEMBER 19, 2024

Committees on Science, Space, and Technology, Homeland Security, and Armed Services discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on July 11, 2023]

A BILL

To improve the cybersecurity of the Federal Government, 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; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Federal Information Security Modernization Act of 2024".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act, unless otherwise specified:

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

(2) 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 Accountability of the House of Representatives; and

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

(3) AWARDEE.—The term "awardee" has the meaning given the term in section 3591 of title 44, United States Code, as added by this Act.

(4) CONTRACTOR.—The term "contractor" has the meaning given the term in section 3591 of title 44, United States Code, as added by this Act.

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

(6) FEDERAL INFORMATION SYSTEM.—The term "Federal information system" has the meaning given the term in section 3591 of title 44, United States Code, as added by this Act.

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

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

(9) 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.

(10) THREAT HUNTING.—The term "threat hunting" means proactively and iteratively searching systems for threats and vulnerabilities, including threats or vulnerabilities that may evade detection by automated threat detection systems.

(11) ZERO TRUST ARCHITECTURE.—The term "zero trust architecture" has the meaning given the term in Special Publication 800–207 of the National Institute of Standards and Technology, or any successor document.

SEC. 3. AMENDMENTS TO TITLE 44.

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

(1) in section 3504—

(A) in subsection (a)(1)(B)—

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

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

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

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

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

(B) in subsection (g)—

(i) by redesignating paragraph (2) as paragraph (3); and

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

"(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, disclosure, and sharing of information collected or maintained by or for agencies;

"(2) in consultation with the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on security, of information collected or maintained by or for agencies; and";

(2) in section 3505—

(A) by striking the first subsection designated as subsection (c);

(B) in paragraph (2) of the second subsection designated as subsection (c), by inserting "an identification of internet accessible information systems and" after "an inventory under this subsection shall include";

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

(i) in subparagraph (B)—

(I) by inserting "the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and" before "the Comptroller General"; and

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

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

(iii) by adding at the end the following:

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

(3) in section 3506—

(A) in subsection (a)(3), by inserting "In carrying out these duties, the Chief Information Officer shall consult, 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 (h)(3), by inserting "security," after "efficiency,"; and

(D) by adding at the end the following:

"(j)(1) Notwithstanding paragraphs (2) and (3) of subsection (a), the head of each agency shall, in accordance with section 522(a) of division H of the Consolidated Appropriations Act, 2005 (42 U.S.C. 2000ee–2), designate a Chief Privacy Officer with the necessary skills, knowledge, and expertise, who shall have the authority and responsibility to—

"(A) lead the privacy program of the agency; and

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

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

"(A) serve in a central leadership position within the agency;

"(B) have visibility into relevant agency operations; and

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

"(3) A privacy officer of an agency established under a statute enacted before the date of enactment of the Federal Information Security Modernization Act of 2024 may carry out the responsibilities under this subsection for the agency."; 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 Secretary of Homeland Security and 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 (2), (3), (4), (5), (6), and (7) as paragraphs (3), (4), (5), (6), (8), and (10), respectively;

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

"(2) The term 'high value asset' means information or an information system that the head of an agency, using policies, principles, standards, or

guidelines issued by the Director under section 3553(a), determines to be so critical to the agency that the loss or degradation of the confidentiality, integrity, or availability of such information or information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.";

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

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

(D) in paragraph (8)(A), as so redesignated, in the matter preceding clause (i), by striking "used" and inserting "owned, managed,";

(E) by inserting after paragraph (8), as so redesignated, the following:

"(9) The term 'penetration test'—

"(A) means an authorized assessment that emulates attempts to gain unauthorized access to, or disrupt the operations of, an information system or component of an information system; and

"(B) includes any additional meaning given the term in policies, principles, standards, or guidelines issued by the Director under section 3553(a)."; and

(F) by inserting after paragraph (10), as so redesignated, the following:

"(11) The term 'shared service' means a centralized mission capability or consolidated business function that is provided to multiple organizations within an agency or to multiple agencies.

"(12) The term 'zero trust architecture' has the meaning given the term in Special Publication 800–207 of the National Institute of Standards and Technology, or any successor document.".

(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(c)(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)(8)(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 3068.—Section 3068(b) of title 10, United States Code, is amended by striking "section 3552(b)(6)" and inserting "section 3552(b)".

(iv) SECTION 3252.—Section 3252(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)(8)(A)(i)".

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a(5)) 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 931(b)(3) (10 U.S.C. 2223 note), by striking "section 3542(b)(2)" and inserting "section 3552(b)"; and

(ii) 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 Na-

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

(i) in subsection (a)(2), by striking "section 3552(b)(6)" and inserting "section 3552(b)"; and

(ii) in subsection (f)—

(I) in paragraph (2), 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 presumption of compromise and least privilege principles, such as zero trust architecture, to improve resiliency and timely response actions to incidents on Federal systems.";

(B) in subsection (b)—

(i) in the matter preceding paragraph (1), by inserting "and the National Cyber Director" after "Director";

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

(iii) by redesignating paragraphs (8) and (9) as paragraphs (10) and (11), respectively; and

(iv) by inserting after paragraph (7) the following:

"(8) expeditiously seeking opportunities to reduce costs, administrative burdens, and other barriers to information technology security and modernization for agencies, including through shared services (and appropriate commercial off the shelf options for such

shared services) for cybersecurity capabilities identified as appropriate by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and other agencies as appropriate;";

(C) in subsection (c)—

(i) in the matter preceding paragraph (1)—

(I) by striking "each year" and inserting "each year during which agencies are required to submit reports under section 3554(c)";

(II) by inserting ", which shall be unclassified but may include 1 or more annexes that contain classified or other sensitive information, as appropriate" after "a report"; and

(III) by striking "preceding year" and inserting "preceding 2 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 the risks and trends identified in the Federal risk assessment required under subsection (i); and";

(D) in subsection (h)—

(i) in paragraph (2)—

(I) in subparagraph (A), by inserting "and the National Cyber Director" after "in coordination with the Director";

(II) in subparagraph (B), by inserting ", the scope of the required action (such as applicable software, firmware, or hardware versions)," after "reasons for the required action"; and

(III) in subparagraph (D), by inserting ", the National Cyber Director," after "notify the Director"; and

(ii) in paragraph (3)(A)(iv), by inserting ", the National Cyber Director" after "the Secretary provides prior notice to the Director";

(E) by amending subsection (i) to read as follows:

"(i) FEDERAL RISK ASSESSMENT.—On an ongoing and continual basis, the Director of the Cybersecurity and Infrastructure Security Agency shall assess the 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 such assessment, including—

"(1) the status of agency cybersecurity remedial actions for high value assets 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 required under section 3554(a)(1)(A);

"(10) relevant reports from inspectors general of agencies and the Government Accountability Office; and

"(11) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant."; and

(F) by adding at the end the following:

"(m) DIRECTIVES.—

"(1) EMERGENCY DIRECTIVE UPDATES.—If the Secretary issues an emergency directive under this section, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives an update on the status of the implementation of the emergency directive at agencies not later than 7 days after the date on which the emergency directive requires an agency to complete a requirement specified by the emergency directive, and every 30 days thereafter until—

"(A) the date on which every agency has fully implemented the emergency directive;

"(B) the Secretary determines that an emergency directive no longer requires active reporting from agencies or additional implementation; or

"(C) the date that is 1 year after the issuance of the directive.

"(2) BINDING OPERATIONAL DIRECTIVE UPDATES.—If the Secretary issues a binding operational directive under this section, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives an update on the status of the implementation of the binding operational directive at agencies not later than 30 days after the issuance of the binding operational directive, and every 90 days thereafter until—

"(A) the date on which every agency has fully implemented the binding operational directive;

"(B) the Secretary determines that a binding operational directive no longer requires ac-

tive reporting from agencies or additional implementation; or

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

"(3) REPORT.—If the Director of the Cybersecurity and Infrastructure Security Agency ceases submitting updates required under paragraphs (1) or (2) on the date described in paragraph (1)(C) or (2)(C), the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Director, the National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a list of every agency that, at the time of the report—

"(A) has not completed a requirement specified by an emergency directive; or

"(B) has not implemented a binding operational directive.

"(n) REVIEW OF OFFICE OF MANAGEMENT AND BUDGET GUIDANCE AND POLICY.—

"(1) CONDUCT OF REVIEW.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget shall review the efficacy of the guidance and policy promulgated by the Director

in reducing cybersecurity risks, including a consideration of reporting and compliance burden on agencies.

"(2) CONGRESSIONAL NOTIFICATION.—The Director of the Office of Management and Budget shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Accountability of the House of Representatives of the results of the review under paragraph (1).

"(3) GAO REVIEW.—The Government Accountability Office shall review guidance and policy promulgated by the Director to assess its efficacy in risk reduction and burden on agencies.

"(o) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard or guideline pursuant to paragraphs (2) or (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 specifications to enable the automated verification of the implementation of the controls.

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

(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 continual basis, assessing agency system risk, as applicable, by—

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

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

"(iii) identifying whether the agency is participating in federally offered cybersecurity shared services programs;

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

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

"(vi) evaluating 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;

"(vii) assessing the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (v) and the agency systems identified under clause (iv); and

"(viii) assessing 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 information from the assessment required 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;

(V) in subparagraph (D), as so redesignated, by inserting "and" after the semicolon at the end; and

(VI) by adding at the end the following:

"(E) providing an update on the ongoing and continual assessment required under subparagraph (A)—

"(i) upon request, to the inspector general of the agency or the Comptroller General of the United States; and

"(ii) at intervals determined by guidance issued by the Director, and to the extent appropriate and practicable using automation, to—

"(I) the Director;

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

"(III) the National Cyber Director;";

(ii) in paragraph (2)—

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

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

(iii) in paragraph (3)(A)—

(I) in the matter preceding clause (i), by striking "senior agency information security officer" and inserting "Chief Information Security Officer";

(II) in clause (i), by striking "this section" and inserting "subsections (a) through (c)";

(III) in clause (ii), by striking "training and" and inserting "skills, training, and";

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

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

"(iii) manage information security, cybersecurity budgets, and risk and compliance activities and explain those concepts to the head of the agency and the executive team of the agency;"; and

(VI) in clause (iv), as so redesignated, by striking "information security duties as that official's primary duty" and inserting "information, computer network, and technology security duties as the Chief Information Security Officers' primary duty";

(iv) in paragraph (5), by striking "annually" and inserting "not less frequently than quarterly"; and

(v) in paragraph (6), by striking "official delegated" and inserting "Chief Information Security Officer delegated";

(B) in subsection (b)—

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

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

(ii) in paragraph (2)—

(I) by striking subparagraph (B);

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

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

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

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

"(iii) binding operational directives and emergency directives issued by the Secretary under section 3553;"; and

(cc) in clause (iv), as so redesignated, by striking "as deter-

mined by the agency;" and inserting "as determined by the agency, considering the agency risk assessment required 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 securely providing the status of remedial cybersecurity actions and un-remediated identified system vulnerabilities of high value assets to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data as appropriate;"; 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 (II), by adding "and" at the end;

(bb) by striking subclause (III); and

(cc) by redesignating subclause (IV) as subclause (III); and

(C) in subsection (c)—

(i) by redesignating paragraph (2) as paragraph (4);

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

"(1) BIENNIAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2024 and not less frequently than once every 2 years thereafter, using the ongoing and continual agency system risk assessment required under subsection (a)(1)(A), the head of each agency shall submit to the Director, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, the Comptroller General of the United States, 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 Accountability 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, and the appropriate authorization and appropriations committees of Congress a report that—

"(A) summarizes the agency system risk assessment required 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 required 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 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; and

"(D) includes the cybersecurity shared services offered by the Cybersecurity and Infrastructure Security Agency that the agency participates in, if any, and explanations for any non-participation in such services.

"(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 1 or more annexes that contain classified or other sensitive information, as appropriate.

"(3) 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 (4), as so redesignated, by striking the period at the end and inserting ", including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section.";

(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 performing, or reviewing the results of, agency 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) 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).";

(F) by striking subsection (j) and inserting the following:

"(j) GUIDANCE.—

"(1) IN GENERAL.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of risk-based guidance for evaluating the effectiveness of an information security program and practices.

"(2) PRIORITIES.—The risk-based guidance developed under paragraph (1) shall include—

"(A) the identification of the most common successful threat patterns;

"(B) the identification of security controls that address the threat patterns described in subparagraph (A);

"(C) any other security risks unique to Federal systems; and

"(D) any other element the Director determines appropriate."; and

(G) by adding at the end the following:

"(k) COORDINATION.—The head of each agency shall coordinate with the inspector general of the agency, as applicable, to ensure consistent understanding of agency cybersecurity or information security policies for the purpose of evaluations of such policies conducted by the inspector general."; and

(5) in section 3556(a)—

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

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

(d) CONFORMING AMENDMENTS.—

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

"3555. Independent evaluation.".

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

(A) in paragraph (1)(B), in the matter preceding clause (i), by striking "annually thereafter" and inserting "thereafter during the years during which a report is required to be sub-

mitted under section 3553(c) of title 44, United States Code"; and

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

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

(ii) by striking "the report required under section 3553(c) of title 44, United States Code" and inserting "that report".

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

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

"SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

"§ 3591. Definitions

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

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

"(1) APPROPRIATE REPORTING ENTITIES.—The term 'appropriate reporting entities' means—

"(A) the majority and minority leaders of the Senate;

"(B) the Speaker and minority leader of the House of Representatives;

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

"(D) the Committee on Commerce, Science, and Transportation of the Senate;

"(E) the Committee on Oversight and Accountability of the House of Representatives;

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

"(G) the Committee on Science, Space, and Technology of the House of Representatives;

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

"(I) the Director;

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

"(K) the National Cyber Director;

"(L) the Comptroller General of the United States; and

"(M) the inspector general of any impacted agency.

"(2) AWARDEE.—The term 'awardee', with respect to an agency—

"(A) means—

"(i) the recipient of a grant from an agency;

"(ii) a party to a cooperative agreement with an agency; and

"(iii) a party to an other transaction agreement with an agency; and

"(B) includes a subawardee of an entity described in subparagraph (A).

"(3) BREACH.—The term 'breach'—

"(A) means the compromise, unauthorized disclosure, unauthorized acquisition, or loss of control of personally identifiable information

owned, maintained or otherwise controlled by an agency, or any similar occurrence; and

"(B) includes any additional meaning given the term in policies, principles, standards, or guidelines issued 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 that creates, collects, stores, processes, maintains, or transmits Federal information on behalf of an agency.

"(5) FEDERAL INFORMATION.—The term 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form.

"(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system owned, managed, or operated by an agency, or on behalf of an agency by a contractor, an awardee, or another organization.

"(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) DEFINITION.—In this section, the term 'covered breach' means a breach—

"(1) involving not less than 50,000 potentially affected individuals; or

"(2) the result of which the head of an agency determines that notifying potentially affected individuals is necessary pursuant to subsection (b)(1), regardless of whether—

"(A) the number of potentially affected individuals is less than 50,000; or

"(B) the notification is delayed under subsection (d).

"(b) 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 Information Officer and Chief Privacy Officer of the agency and, as appropriate, any non-Federal entity supporting the remediation of the breach, shall—

"(1) determine whether notice to any individual potentially affected by the breach is appropriate, including by conducting 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) if the head of the agency determines notification is necessary pursuant to paragraph (1), provide written notification in accordance with subsection (c) 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.

"(c) CONTENTS OF NOTIFICATION.—Each notification of a breach provided to an individual under subsection (b)(2) shall include, to the maximum extent practicable—

"(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 the appropriate 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.

"(d) DELAY OF NOTIFICATION.—

"(1) IN GENERAL.—The head of an agency, in coordination with the Director and the National Cyber Director, and as appropriate, the Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security, may delay a notification required under subsection (b) or (e) if the notification would—

"(A) impede a criminal investigation or a national security activity;

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

"(C) reveal sensitive sources and methods;

"(D) cause damage to national security; or

"(E) hamper security remediation actions.

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

"(3) NATIONAL SECURITY SYSTEMS.—The head of an agency delaying notification under this subsection with respect to a breach exclusively of a national security system shall coordinate such delay with the Secretary of Defense.

"(e) 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 (b)(1), or that it is necessary to update the details of the information provided to potentially affected individuals as described in subsection (c), 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 (b) of those changes.

"(f) DELAY OF NOTIFICATION REPORT.—

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

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

"(g) CONGRESSIONAL REPORTING REQUIREMENTS.—

"(1) REVIEW AND UPDATE.—On a periodic basis, the Director of the Office of Management and Budget shall review, and update as appropriate, breach notification policies and guidelines for agencies.

"(2) REQUIRED NOTICE FROM AGENCIES.—Subject to paragraph (4), the Director of the Office of Management and Budget shall require the head of an agency affected by a covered breach to expeditiously and not later than 30 days after the date on which the agency discovers the covered breach give notice of the breach, which may be provided electronically, to—

"(A) each congressional committee described in section 3554(c)(1); and

"(B) the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

"(3) CONTENTS OF NOTICE.—Notice of a covered breach provided by the head of an agency pursuant to paragraph (2) shall include, to the extent practicable—

"(A) information about the covered breach, including a summary of any information about how the covered breach occurred known by the agency as of the date of the notice;

"(B) an estimate of the number of individuals affected by the covered breach based on information known by the agency as of the date of the notice, including an assessment of the risk of harm to affected individuals;

"(C) a description of any circumstances necessitating a delay in providing notice to individuals affected by the covered breach in accordance with subsection (d); and

"(D) an estimate of when the agency will provide notice to individuals affected by the covered breach, if applicable.

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

"(A) the majority and minority leaders of the Senate;

"(B) the Speaker and minority leader of the House of Representatives;

"(C) the appropriations committees of Congress;

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

"(E) the Select Committee on Intelligence of the Senate;

"(F) the Committee on Oversight and Accountability of the House of Representatives; and

"(G) the Permanent Select Committee on Intelligence of the House of Representatives.

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

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

"(1) limit—

"(A) the authority of the Director to issue guidance relating to notifications of, or the head of an agency to notify individuals potentially affected by, breaches that are not determined to be covered breaches or major incidents;

"(B) the authority of the Director to issue guidance relating to notifications and reporting of breaches, covered breaches, or major incidents;

"(C) the authority of the head of an agency to provide more information than required under subsection (b) when notifying individuals potentially affected by a breach;

"(D) the timing of incident reporting or the types of information included in incident reports provided, pursuant to this subchapter, to—

"(i) the Director;

"(ii) the National Cyber Director;

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

"(iv) any other agency;

"(E) the authority of the head of an agency to provide information to Congress about agency breaches, including—

"(i) breaches that are not covered breaches; and

"(ii) additional information beyond the information described in subsection (g)(3); or

"(F) any congressional reporting requirements of agencies under any other law; or

"(2) limit or supersede any existing privacy protections in existing law.

"§ 3593. Congressional and executive branch reports on major incidents

"(a) APPROPRIATE CONGRESSIONAL ENTITIES.—In this section, the term 'appropriate congressional entities' means—

"(1) the majority and minority leaders of the Senate;

"(2) the Speaker and minority leader of the House of Representatives;

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

"(4) the Committee on Commerce, Science, and Transportation of the Senate;

"(5) the Committee on Oversight and Accountability of the House of Representatives;

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

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

"(8) the appropriate authorization and appropriations committees of Congress.

"(b) INITIAL NOTIFICATION.—

"(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 notification, which may be submitted electronically and include 1 or more annexes that contain classified or other sensitive information, as appropriate.

"(2) CONTENTS.—A notification required under paragraph (1) with respect to a major incident shall include the following, based on information available to agency officials as of the date on which the agency submits the notification:

"(A) A summary of the information available about the major incident, including how the major incident occurred and the threat causing the major incident.

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

"(i) the breach was the reason the incident was determined to be a major incident; and

"(ii) head of the agency determined it was appropriate to provide notification to potentially impacted individuals pursuant to section 3592(b)(1).

"(C) A preliminary assessment of the impacts to—

"(i) the agency;

"(ii) the Federal Government;

"(iii) the national security, foreign relations, homeland security, and economic security of the United States; and

"(iv) the civil liberties, public confidence, privacy, and public health and safety of the people of the United States.

"(D) If applicable, whether any ransom has been demanded or paid, or is expected to be paid, by any entity operating a Federal information system or with access to Federal information or a Federal information system, including, as available, the name of the entity demanding ransom, the date of the demand, and the amount and type of currency demanded, unless disclosure of such information will disrupt an active Federal law enforcement or national security operation.

"(c) SUPPLEMENTAL UPDATE.—Within a reasonable amount of time, but not later than 30 days after the date on which the head of an agency submits a written notification under subsection (b), the head of the agency shall provide to the appropriate congressional entities an unclassified and written update, which may include 1 or more annexes that contain classified or other sensitive information, as appropriate, on the major incident, based on informa-

tion available to agency officials as of the date on which the agency provides the update, on—

"(1) system vulnerabilities relating to the major incident, where applicable, means by which the major incident occurred, the threat causing the major incident, where applicable, and impacts of the major incident to—

"(A) the agency;

"(B) other Federal agencies, Congress, or the judicial branch;

"(C) the national security, foreign relations, homeland security, or economic security of the United States; or

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

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

"(3) if the major incident involved a breach, a description of the affected information, an estimate of the number of individuals potentially impacted, and any assessment to the risk of harm to such individuals;

"(4) 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;

"(5) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d), if applicable;

"(6) as appropriate and available, actions undertaken by any non-Federal entities impacted by or supporting remediation of the major incident; and

"(7) as appropriate and available, recommendations for mitigating future similar incidents, including recommendations from any non-Federal entity impacted by or supporting the remediation of the major incident.

"(d) ADDITIONAL UPDATE.—If the head of an agency, the Director, or the National Cyber Director determines that there is any significant change in the understanding of the scope, scale, or consequence of a major incident for which the head of the agency submitted a written notification and update under subsections (b) and (c), the head of the agency shall submit to the appropriate congressional entities a written update that includes information relating to the change in understanding.

"(e) BIENNIAL REPORT.—Each agency shall submit as part of the biennial report required under section 3554(c)(1) a description of each major incident that occurred during the 2-year period preceding the date on which the biennial report is submitted.

"(f) REPORT DELIVERY.—

"(1) IN GENERAL.—Any written notification or update required to be submitted under this section—

"(A) shall be submitted in an electronic format; and

"(B) may be submitted in a paper format.

"(2) CLASSIFICATION STATUS.—Any written notification or update required to be submitted under this section—

"(A) shall be—

"(i) unclassified; and

"(ii) submitted through unclassified electronic means pursuant to paragraph (1)(A); and

"(B) may include classified annexes, as appropriate.

"(g) REPORT CONSISTENCY.—To achieve consistent and coherent agency reporting to Congress, the National Cyber Director, in coordination with the Director, shall—

"(1) provide recommendations to agencies on formatting and the contents of information to be included in the reports required under this section, including recommendations for consistent formats for presenting any associated metrics; and

"(2) maintain a comprehensive record of each major incident notification, update, and briefing provided under this section, which shall—

"(A) include, at a minimum—

"(i) the full contents of the written notification or update;

"(ii) the identity of the reporting agency; and

"(iii) the date of submission; and

"(iv) a list of the recipient congressional entities; and

"(B) be made available upon request to 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, and the Committee on Oversight and Accountability of the House of Representatives.

"(h) NATIONAL SECURITY SYSTEMS CONGRESSIONAL REPORTING EXEMPTION.—With respect to a major incident

that occurs exclusively on a national security system, the head of the affected agency shall submit the notifications and reports required to be submitted to Congress under this section only to—

"(1) the majority and minority leaders of the Senate;

"(2) the Speaker and minority leader of the House of Representatives;

"(3) the appropriations committees of Congress;

"(4) the appropriate authorization committees of Congress;

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

"(6) the Select Committee on Intelligence of the Senate;

"(7) the Committee on Oversight and Accountability of the House of Representatives; and

"(8) the Permanent Select Committee on Intelligence of the House of Representatives.

"(i) MAJOR INCIDENTS INCLUDING BREACHES.—If a major incident constitutes a covered breach, as defined in section 3592(a), information on the covered breach required to be submitted to Congress pursuant to section 3592(g) may—

"(1) be included in the notifications required under subsection (b) or (c); or

"(2) be reported to Congress under the process established under section 3592(g).

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

"(1) limit—

"(A) the ability of an agency to provide additional reports or briefings to Congress;

"(B) Congress from requesting additional information from agencies through reports, briefings, or other means; and

"(C) any congressional reporting requirements of agencies under any other law; or

"(2) limit or supersede any privacy protections under any other law.

"§ 3594. Government information sharing and incident response

"(a) IN GENERAL.—

"(1) INCIDENT SHARING.—Subject to paragraph (4) and subsection (b), and in accordance with the applicable requirements pursuant to section 3553(b)(2)(A) for reporting to the Federal information security incident center established under section 3556, the head of each agency shall provide to the Cy-

bersecurity and Infrastructure Security Agency information relating to any incident affecting the agency, whether the information is obtained by the Federal Government directly or indirectly.

"(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall include, at a minimum—

"(A) a full description of the incident, including—

"(i) all indicators of compromise and tactics, techniques, and procedures;

"(ii) an indicator of how the intruder gained initial access, accessed agency data or systems, and undertook additional actions on the network of the agency;

"(iii) information that would support enabling defensive measures; and

"(iv) other information that may assist in identifying other victims;

"(B) information to help prevent similar incidents, such as information about relevant safeguards in place when the incident occurred and the effectiveness of those safeguards; and

"(C) 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 any malicious actor that may have conducted or caused the incident, subject to appropriate privacy protections.

"(3) INFORMATION SHARING.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

"(A) make incident information provided under paragraph (1) available to the Director and the National Cyber Director;

"(B) to the greatest extent practicable, share information relating to an incident with—

"(i) the head of any agency that may be—

"(I) impacted by the incident;

"(II) particularly susceptible to the incident; or

"(III) similarly targeted by the incident; and

"(ii) appropriate Federal law enforcement agencies to facilitate any necessary threat response activities, as requested;

"(C) coordinate any necessary information sharing efforts relating to a major incident with the private sector; and

"(D) notify the National Cyber Director of any efforts described in subparagraph (C).

"(4) NATIONAL SECURITY SYSTEMS EXEMPTION.—

"(A) IN GENERAL.—Notwithstanding paragraphs (1) and (3), each agency operating or exercising control of a national security system shall share information about an incident that occurs exclusively on a national security system with the Secretary of Defense, the Director, the National Cyber Director, and 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) PROTECTIONS.—Any information sharing and handling of information under this paragraph shall be appropriately protected con-

sistent with procedures authorized for the protection of sensitive sources and methods or by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

"(b) AUTOMATION.—In providing information and selecting a method to provide information under subsection (a), the head of each agency shall implement subsection (a)(1) in a manner that provides such information to the Cybersecurity and Infrastructure Security Agency in an automated and machine-readable format, to the greatest extent practicable.

"(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to suspect or conclude that a major incident occurred involving Federal information in electronic medium or form that does not exclusively involve a national security system shall coordinate with—

"(1) the Cybersecurity and Infrastructure Security Agency to facilitate asset response activities and provide recommendations for mitigating future incidents; and

"(2) consistent with relevant policies, appropriate Federal law enforcement agencies to facilitate threat response activities.

"§ 3595. Responsibilities of contractors and awardees

"(a) NOTIFICATION.—

"(1) IN GENERAL.—Any contractor or awardee of an agency shall provide written notification to the agency if the contractor or awardee has a reasonable basis to conclude that—

"(A) an incident or breach has occurred with respect to Federal information the contractor or awardee collected, used, or maintained on behalf of an agency;

"(B) an incident or breach has occurred with respect to a Federal information system used, operated, managed, or maintained on behalf of an agency by the contractor or awardee;

"(C) a component of any Federal information system operated, managed, or maintained by a contractor or awardee contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, for which there is reliable evidence of a successful exploitation of the vulnerability

by an actor without authorization of the Federal information system owner; or

"(D) the contractor or awardee has received from the agency personally identifiable information or personal health information that is beyond the scope of the contract or agreement with the agency that the contractor or awardee is not authorized to receive.

"(2) THIRD-PARTY NOTIFICATION OF VULNERABILITIES.—Subject to the guidance issued by the Director pursuant to paragraph (4), any contractor or awardee of an agency shall provide written notification to the agency and the Cybersecurity and Infrastructure Security Agency if the contractor or awardee has a reasonable basis to conclude that a component of any Federal information system operated, managed, or maintained on behalf of an agency by the contractor or awardee on behalf of the agency contains a security vulnerability, including a supply chain compromise or an identified software or hardware vulnerability, that has been reported to the contractor or awardee by a third party, including through a vulnerability disclosure program.

"(3) PROCEDURES.—

"(A) SHARING WITH CISA.—As soon as practicable following a notification of an incident or vulnerability to an agency by a contractor or awardee under paragraph (1), the head of the agency shall provide, pursuant to section 3594, information about the incident or vulnerability to the Director of the Cybersecurity and Infrastructure Security Agency.

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

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

"(ii) make a notification required under paragraph (2) within a reasonable time, but not later than 90 days after the date on which the contractor or awardee has reasonable basis to suspect or conclude that

the criteria under paragraph (2) have been met.

"(C) PROCEDURES.—Following a notification of a breach or incident to an agency by a contractor or awardee under paragraph (1), the head of the agency, in consultation with the contractor or awardee, shall carry out the applicable requirements under sections 3592, 3593, and 3594 with respect to the breach or incident.

"(D) RULE OF CONSTRUCTION.—Nothing in subparagraph (B) shall be construed to allow the negation of the requirements to notify vulnerabilities under paragraph (1) or (2) through a contract, grant, cooperative agreement, or other transaction agreement.

"(4) GUIDANCE.—The Director shall issue guidance as soon as practicable to agencies relating to the scope of vulnerabilities to be included in required notifications under paragraph (2), such as the minimum severity or minimum risk level of a vulnerability included in required notifications, whether vulnerabilities that are already publicly disclosed must be reported, or likely cybersecurity impact to Federal information systems.

"(b) REGULATIONS; MODIFICATIONS.—

"(1) IN GENERAL.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2024—

"(A) the Federal Acquisition Regulatory Council shall promulgate regulations, as appropriate, relating to the responsibilities of contractors and recipients of other transaction agreements and cooperative agreements to comply with this section; and

"(B) the Office of Federal Financial Management shall promulgate regulations under title 2, Code of Federal Regulations, as appropriate, relating to the responsibilities of grantees to comply with this section.

"(2) IMPLEMENTATION.—Not later than 1 year after the date on which the Federal Acquisition Regulatory Council and the Office of Federal Financial Management promulgates regulations under paragraph (1), the head of each agency shall implement policies and procedures, as appropriate, necessary to implement those regulations.

"(3) CONGRESSIONAL NOTIFICATION.—

"(A) IN GENERAL.—The head of each agency head shall notify the Director upon implementation of policies and procedures necessary to

implement the regulations promulgated under paragraph (1).

"(B) OMB NOTIFICATION.— Not later than 30 days after the date described in paragraph (2), the Director shall notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives on the status of the implementation by each agency of the regulations promulgated under paragraph (1).

"(c) ALLOWABLE USE.—Information provided to an agency pursuant to this section may be disclosed to, retained by, and used by any agency, component, officer, employee, or agent of the Federal Government solely for any of the following:

"(1) A cybersecurity purpose (as defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)).

"(2) Identifying—

"(A) a cyber threat (as defined in such section 2200), including the source of the cyber threat; or

"(B) a security vulnerability (as defined in such section 2200).

"(3) Preventing, investigating, disrupting, or prosecuting an offense arising out of an incident notified to an agency pursuant to this section or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

"(d) HARMONIZATION OF OTHER PRIVATE-SECTOR CYBERSECURITY REPORTING OBLIGATIONS.—Any non-Federal entity required to report an incident under section 2242 of the Homeland Security Act of 2002 (6 U.S.C. 681b) may submit as part of the written notification requirements in this section all information required by such section 2242 to the agency of which the entity is a contractor or recipient of Federal financial assistance, or with which the entity holds an other transaction agreement or cooperative agreement, within the deadline specified in subsection (a)(3)(B)(1). If such submission is completed, the non-Federal entity shall not be required to subsequently report the same incident under the requirements of such section 2242. Any incident information shared under this subsection shall be shared with the Director of the Cybersecurity and Infrastructure Security Agency pursuant to subsection (a)(3)(A).

"(e) NATIONAL SECURITY SYSTEMS EXEMPTION.—Notwithstanding any other provision of this section, a contractor or awardee of an agency that would be required to

report an incident or vulnerability pursuant to this section that occurs exclusively on a national security system shall—

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

"(2) comply with applicable laws and policies relating to national security systems.

"§ 3596. Training

"(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to a Federal information system because of the status of the individual as—

"(1) an employee, contractor, awardee, volunteer, or intern of an agency; or

"(2) an employee of a contractor or awardee of an agency.

"(b) BEST PRACTICES AND CONSISTENCY.—The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, the National Cyber Director, and the Director of the National Institute of Standards and Technology, shall consolidate best practices to support consistency across agencies in cybersecurity incident response training, including—

"(1) information to be collected and shared with the Cybersecurity and Infrastructure Security Agency

pursuant to section 3594(a) and processes for sharing such information; and

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

"(c) AGENCY TRAINING.—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 any suspected or confirmed incident involving Federal information in any medium or form, including paper, oral, and electronic.

"(d) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (c) may be included as part of an annual privacy, security awareness, or other appropriate 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 perform and, in coordination with the Director and the National Cyber Director, develop, continuous monitoring and quan-

titative and qualitative analyses of incidents at agencies, including major incidents, including—

"(A) the causes of incidents, including—

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

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

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

"(C) 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 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 ex-

tent practicable, use machine-readable data, automation, and machine learning processes.

"(3) SHARING OF DATA AND ANALYSIS.—

"(A) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall share on an ongoing basis the analyses and underlying data required under this subsection with agencies, the Director, 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 of the Cybersecurity and Infrastructure Security Agency shall share the analyses—

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

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

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

"(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, 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;

"(B) the total number of incidents of the agency; and

"(C) 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.—

"(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency shall make a version of each report submitted under subsection (b) publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year during which the report is submitted.

"(2) EXEMPTION.—The publication requirement under paragraph (1) shall not apply to a portion of a report that contains content that should be protected in the interest of national security, as determined by the Director, the Director of the Cybersecurity and Infrastructure Security Agency, or the National Cyber Director.

"(3) LIMITATION ON EXEMPTION.—The exemption under paragraph (2) shall not apply to any version of a report submitted to the appropriate reporting entities under subsection (b).

"(4) REQUIREMENT FOR COMPILING INFORMATION.—

"(A) COMPILATION.—Subject to subparagraph (B), in making a report publicly available under paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information so that no specific incident of an agency can be identified.

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

"(i) with the concurrence of the Director and the National Cyber Director;

"(ii) in consultation with the impacted agency, which may, as appropriate, consult with any non-Federal entity impacted by or supporting the remediation of such incident; and

"(iii) in consultation with the inspector general of the impacted agency.

"(d) INFORMATION PROVIDED BY AGENCIES.—

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

"(2) NONCOMPLIANCE REPORTS.—During any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes the information described in subsection (b) with respect to the agency.

"(e) NATIONAL SECURITY SYSTEM REPORTS.—

"(1) IN GENERAL.—Notwithstanding any other provision of this section, the Secretary of Defense, in consultation with the Director, the National Cyber Director, the Director of National Intelligence, and the Director of the Cybersecurity and Infrastructure Security Agency shall annually submit a report that includes the information described in subsection (b) with respect to national security systems, 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—

"(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 Select Committee on Intelligence of the Senate;

"(E) the Committee on Armed Services of the Senate;

"(F) the Committee on Appropriations of the Senate;

"(G) the Committee on Oversight and Accountability of the House of Representatives;

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

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

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

"(K) the Committee on Appropriations of the House of Representatives.

"(2) CLASSIFIED FORM.—A report required under paragraph (1) may be submitted in a classified form.

"§ 3598. Major incident definition

"(a) IN GENERAL.—Not later than 1 year after the later of the date of enactment of the Federal Information Security Modernization Act of 2024 and the most recent publication by the Director of guidance to agencies regarding major incidents as of the date of enactment of the Federal Information Security Modernization Act of 2024, the Director shall develop, in coordination with the National Cyber Director, 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 a Federal information system—

"(A) any incident the head of the agency determines is likely to result in demonstrable harm to—

"(i) the national security interests, foreign relations, homeland security, or economic security of the United States; or

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

"(B) any incident the head of the agency determines likely to result in an inability or substantial disruption for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

"(C) any incident the head of the agency determines substantially disrupts or substantially degrades the operations of a high value asset owned or operated by the agency;

"(D) any incident involving the exposure to a foreign entity of sensitive agency information, such as the communications of the head of the agency, the head of a component of the agency, or the direct reports of the head of the agency or the head of a component of the agency; and

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

"(2) stipulate that the National Cyber Director, in consultation with the Director and the Director of the Cybersecurity and Infrastructure Security Agency, may declare a major incident at any agency, and such a declaration shall be considered 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;

"(3) stipulate that, in determining whether an incident constitutes a major incident under the standards described in paragraph (1), the head of the agency shall consult with the National Cyber Director; and

"(4) stipulate that the mere report of a vulnerability discovered or disclosed without a loss of confidentiality, integrity, or availability shall not on its own constitute a major incident.

"(c) EVALUATION AND UPDATES.—Not later than 60 days after the date on which the Director first promulgates the guidance required under subsection (a), and not less frequently than once during the first 90 days of each evenly numbered Congress thereafter, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a briefing that includes—

"(1) an evaluation of any necessary updates to the guidance;

"(2) an evaluation of any necessary updates to the definition of the term 'major incident' included in the guidance; 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. 4. 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 (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.";

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

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

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

"(B) require that any proposal for the use of amounts in the Fund includes, as appropriate, and which may be incorporated into otherwise required project proposal documentation—

"(i) cybersecurity risk management considerations; and

"(ii) a supply chain risk assessment in accordance with section 1326 of title 41."; and

(3) 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,"; and

(B) in subsection (h), by inserting ", including cybersecurity performances," after "the performances"; and

(2) in section 11303(b)(2)(B)—

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

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

(C) by adding at the end the following:

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

(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 11317, by inserting "security," before "or schedule"; and

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

SEC. 5. ACTIONS TO ENHANCE FEDERAL INCIDENT TRANSPARENCY.

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

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

(A) develop a plan for the development, using systems in place on the date of enactment of this Act, 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 of the Cybersecurity and Infrastructure Security Agency anticipates encountering; and

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

(B) provide to the appropriate congressional committees a briefing on the plan developed under subparagraph (A).

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

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

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

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

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

(A) by striking subsections (b) and (d); and

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

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop, and as appropriate update, guidance, on the content, timeliness, and format of the infor-

mation provided by agencies under section 3594(a) of title 44, United States Code, as added by this Act.

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

(i) enable the efficient development of—

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

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

(ii) include requirements for the timeliness of data production.

(C) AUTOMATION.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promote, as feasible, the use of automation and machine-readable data for data sharing under section 3594(a) of title 44, United States Code, as added by this Act.

(3) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall issue guidance to 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 agencies of incidents involving information of the Federal Government.

(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, to the extent necessary, to assist the recipient agency in responding to an incident (as defined in section 3552 of title 44) or

breach (as defined in section 3591 of title 44) or to fulfill the information sharing requirements under section 3594 of title 44.".

SEC. 6. 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 1 year after the date of enactment of this Act, the Director shall develop, in consultation with the National Cyber Director, and issue guidance requiring the head of each agency to notify a reporting entity in an appropriate and timely manner, and take into consideration the need to coordinate with Sector Risk Management Agencies (as defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)), as appropriate, of an incident at the agency 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) any information system (as defined in section 3502 of title 44, United States Code) used in the transmission or storage of the sensitive information described in paragraph (1).

SEC. 7. 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.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies that—

"(1) requires agencies to perform penetration testing on information systems, as appropriate, including on high value assets;

"(2) provides policies governing the development of—

"(A) rules of engagement for using penetration testing; and

"(B) procedures to use the results of penetration testing to improve the cybersecurity and risk management of the agency;

"(3) ensures that operational support or a shared service is available; and

"(4) in no manner restricts the authority of the Secretary of Homeland Security or the Director of the Cybersecurity and Infrastructure Agency to conduct threat hunting pursuant to section 3553, or penetration testing under this chapter.

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

"(c) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (a) shall be delegated to—

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

"(2) the Director of National Intelligence in the case of a system described in section 3553(e)(3).".

(b) EXISTING GUIDANCE.—

(1) IN GENERAL.—Compliance with guidance issued by the Director relating to penetration testing before the date of enactment of this Act shall be

deemed to be compliant with section 3559A of title 44, United States Code, as added by this Act.

(2) IMMEDIATE NEW GUIDANCE NOT REQUIRED.—Nothing in section 3559A of title 44, United States Code, as added by this Act, shall be construed to require the Director to issue new guidance to agencies relating to penetration testing before the date described in paragraph (3).

(3) GUIDANCE UPDATES.—Notwithstanding paragraphs (1) and (2), not later than 2 years after the date of enactment of this Act, the Director shall review and, as appropriate, update existing guidance requiring penetration testing by agencies.

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

"3559A. Federal penetration testing.".

(d) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by this Act, is further amended by inserting after paragraph (8) the following:

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

"(A) without consent or authorization from agencies; and

"(B) with prior consultation with the head of the agency at least 72 hours in advance of such testing;".

SEC. 8. VULNERABILITY DISCLOSURE POLICIES.

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

"§ 3559B. Federal vulnerability disclosure policies

"(a) PURPOSE; SENSE OF CONGRESS.—

"(1) PURPOSE.—The purpose of Federal vulnerability disclosure policies is to create a mechanism to enable the public to inform agencies of vulnerabilities in Federal information systems.

"(2) SENSE OF CONGRESS.—It is the sense of Congress that, in implementing the requirements of this section, the Federal Government should take appropriate steps to reduce real and perceived burdens in communications between agencies and security researchers.

"(b) DEFINITIONS.—In this section:

"(1) CONTRACTOR.—The term 'contractor' has the meaning given the term in section 3591.

"(2) INTERNET OF THINGS.—The term 'internet of things' has the meaning given the term in Special Publication 800–213 of the National Institute of

Standards and Technology, entitled 'IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements', or any successor document.

"(3) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

"(4) SUBMITTER.—The term 'submitter' means an individual that submits a vulnerability disclosure report pursuant to the vulnerability disclosure process of an agency.

"(5) VULNERABILITY DISCLOSURE REPORT.—The term 'vulnerability disclosure report' means a disclosure of a security vulnerability made to an agency by a submitter.

"(c) GUIDANCE.—The Director shall issue guidance to agencies that includes—

"(1) use of the information system security vulnerabilities disclosure process guidelines established under section 4(a)(1) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3b(a)(1));

"(2) direction to not recommend or pursue legal action against a submitter or an individual that conducts a security research activity that—

"(A) represents a good faith effort to identify and report security vulnerabilities in information systems; or

"(B) otherwise represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (f)(2);

"(3) direction on sharing relevant information in a consistent, automated, and machine-readable manner with the Director of the Cybersecurity and Infrastructure Security Agency;

"(4) the minimum scope of agency systems required to be covered by the vulnerability disclosure policy of an agency required under subsection (f)(2), including exemptions under subsection (g);

"(5) requirements for providing information to the submitter of a vulnerability disclosure report on the resolution of the vulnerability disclosure report;

"(6) a stipulation that the mere identification by a submitter of a security vulnerability, without a significant compromise of confidentiality, integrity, or availability, does not constitute a major incident; and

"(7) the applicability of the guidance to internet of things devices owned or controlled by an agency.

"(d) CONSULTATION.—In developing the guidance required under subsection (c)(3), the Director shall consult

with the Director of the Cybersecurity and Infrastructure Security Agency.

''(e) 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;

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

''(4) as appropriate, implement the requirements of this section, in accordance with the authority under section 3553(b)(8), as a shared service available to agencies.

''(f) 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 and to the extent consistent with the security of information systems but with the presumption of disclosure—

''(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, including for internet of things devices owned or controlled by the agency;

"(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;

"(iv) the disclosure policy for a contractor; and

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

"(B) with respect to a vulnerability disclosure report to an agency, describe—

"(i) how the submitter should submit the vulnerability disclosure 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 and cover every internet accessible information system used or operated by that agency or on behalf of that agency.

"(3) IDENTIFIED SECURITY VULNERABILITIES.—The head of each agency shall—

"(A) consider security vulnerabilities reported in accordance with paragraph (2);

"(B) commensurate with the risk posed by the security vulnerability, address such security vulnerability using the security vulnerability management process of the agency; and

"(C) in accordance with subsection (c)(5), provide information to the submitter of a vulnerability disclosure report.

"(g) EXEMPTIONS.—

"(1) IN GENERAL.—The Director and the head of each agency shall carry out this section in a manner

consistent with the protection of national security information.

"(2) LIMITATION.—The Director and the head of each agency may not publish under subsection (f)(1) or include in a vulnerability disclosure policy under subsection (f)(2) host names, services, information systems, or other information that the Director or the head of an agency, in coordination with the Director and other appropriate heads of agencies, determines would—

"(A) disrupt a law enforcement investigation;

"(B) endanger national security or intelligence activities; or

"(C) impede national defense activities or military operations.

"(3) NATIONAL SECURITY SYSTEMS.—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).

"(i) REVISION OF FEDERAL ACQUISITION REGULATION.—The Federal Acquisition Regulation shall be revised as necessary to implement the provisions under this section.".

(b) EXISTING GUIDANCE AND POLICIES.—

(1) IN GENERAL.—Compliance with guidance issued by the Director relating to vulnerability disclosure policies before the date of enactment of this Act shall be deemed to be compliance with section 3559B of title 44, United States Code, as added by this title.

(2) IMMEDIATE NEW GUIDANCE NOT REQUIRED.—Nothing in section 3559B of title 44, United States Code, as added by this title, shall be construed to require the Director to issue new guidance to agencies relating to vulnerability disclosure policies before the date described in paragraph (4).

(3) IMMEDIATE NEW POLICIES NOT REQUIRED.—Nothing in section 3559B of title 44, United States Code, as added by this title, shall be construed to require the head of any agency to issue new policies relating to vulnerability disclosure policies before the issuance of any updated guidance under paragraph (4).

(4) GUIDANCE UPDATE.—Notwithstanding paragraphs (1), (2) and (3), not later than 4 years after the date of enactment of this Act, the Director shall review and, as appropriate, update existing guidance relating to vulnerability disclosure policies.

(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 policies.".

(d) CONFORMING UPDATE AND REPEAL.—

(1) GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES.—Section 5 of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking subsections (d) and (e).

(2) IMPLEMENTATION AND CONTRACTOR COMPLIANCE.—The IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a et seq.) is amended—

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

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

SEC. 9. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) BRIEFINGS.—Not later than 1 year after the date of enactment of this Act, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Accountability and Homeland Security of the House of Representatives a briefing on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from trusted networks to implement security controls based on a presumption of compromise, including through the transition to zero trust architecture;

(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 as quickly as practicable, accounting for intelligence or law enforcement purposes; and

(6) otherwise increasing the resource costs for entities that cause incidents to be successful.

(b) PROGRESS REPORT.—As a part of each report required to be submitted under section 3553(c) of title 44,

United States Code, during the period beginning on the date that is 4 years after the date of enactment of this Act and ending on the date that is 10 years after the date of enactment of this Act, the Director shall include an update on agency implementation of zero trust architecture, which shall include—

(1) a description of steps agencies have 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.

(c) CLASSIFIED ANNEX.—Each update required under subsection (b) may include 1 or more annexes that contain classified or other sensitive information, as appropriate.

(d) NATIONAL SECURITY SYSTEMS.—

(1) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Secretary of Defense shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Accountability of the House of Representatives, the Committee on Armed Services

of the Senate, the Committee on Armed Services of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a briefing on the implementation of zero trust architecture with respect to national security systems.

(2) PROGRESS REPORT.—Not later than the date on which each update is required to be submitted under subsection (b), the Secretary of Defense shall submit to the congressional committees described in paragraph (1) a progress report on the implementation of zero trust architecture with respect to national security systems.

SEC. 10. AUTOMATION AND ARTIFICIAL INTELLIGENCE.

(a) DEFINITION.—In this section, the term "information system" has the meaning given the term in section 3502 of title 44, United States Code.

(b) USE OF ARTIFICIAL INTELLIGENCE.—

(1) IN GENERAL.—As appropriate, the Director shall issue guidance on the use of artificial intelligence by agencies to improve the cybersecurity of information systems.

(2) CONSIDERATIONS.—The Director and head of each agency shall consider the use and capabilities of

artificial intelligence systems in furtherance of the cybersecurity of information systems.

(3) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter until the date that is 5 years after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of artificial intelligence to further the cybersecurity of information systems.

(c) COMPTROLLER GENERAL REPORTS.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the appropriate congressional committees a report on the risks to the privacy of individuals and the cybersecurity of information systems associated with the use by Federal agencies of artificial intelligence systems or capabilities.

(2) STUDY.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall perform a study, and submit to the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate and the Committees on Oversight and Accountability, Homeland Security,

and Science, Space, and Technology of the House of Representatives a report, on the use of automation, artificial intelligence, including generative artificial intelligence, and machine-readable data across the Federal Government for cybersecurity purposes, including—

(A) 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, as amended by this Act; and

(B) to combat social engineering attacks.

SEC. 11. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) CODIFYING FEDERAL CYBERSECURITY REQUIREMENTS IN TITLE 44.—

(1) AMENDMENT TO FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—Section 225 of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523) is amended by striking subsections (b) and (c).

(2) TITLE 44.—Section 3554 of title 44, United States Code, as amended by this Act, is further amended by adding at the end the following:

"(f) SPECIFIC CYBERSECURITY REQUIREMENTS AT AGENCIES.—

"(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under this subchapter, and except as provided under paragraph (3), the head of each agency shall—

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

"(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and the need of individuals to access the data;

"(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

"(D) implement identity and access management systems to ensure the security of Federal information systems and protect agency records and data from fraud resulting from the misrepresentation of identity or identity theft, including—

"(i) a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires, at a

minimum, user authentication and verification services consistent with applicable law and guidance issued by the Director of the Office of Management and Budget who shall consider any applicable standard or guideline developed by the National Institute of Standards and Technology, which may be one developed by the Administrator of General Services in consultation with the Director of the Office of Management and Budget; and

"(ii) multi-factor authentication, consistent with guidance issued by the Director of the Office of Management and Budget who shall consider any applicable standard or guideline developed by the National Institute of Standards and Technology, for—

"(I) remote access to an information system; and

"(II) each user account with elevated privileges on an information system.

"(2) PROHIBITION.—

"(A) DEFINITION.—In this paragraph, the term 'internet of things' has the meaning given the term in section 3559B.

"(B) PROHIBITION.—Consistent with policies, standards, guidelines, and directives on information security under this subchapter, and except as provided under paragraph (3), the head of an agency may not procure, obtain, renew a contract to procure or obtain in any amount, notwithstanding section 1905 of title 41, or use an internet of things device if the Chief Information Officer of the agency determines during a review required under section 11319(b)(1)(C) of title 40 of a contract for an internet of things device that the use of the device prevents compliance with the standards and guidelines developed under section 4 of the IoT Cybersecurity Improvement Act (15 U.S.C. 278g–3b) with respect to the device.

"(3) EXCEPTIONS.—

"(A) IN GENERAL.—The requirements under subparagraphs (A), (B), (C), and (D)(ii) of paragraph (1) shall not apply to an information system for which the head of the agency, without delegation, has—

"(i) certified to the Director with particularity that—

"(I) operational requirements articulated in the certification and related to the information system would make it excessively burdensome to implement the cybersecurity requirement;

"(II) the cybersecurity requirement is not necessary to secure the information system or agency information stored on or transiting it; and

"(III) the agency has taken all necessary steps to secure the information system and agency information stored on or transiting it; and

"(ii) submitted the certification described in clause (i) to the appropriate congressional committees and the authorizing committees of the agency.

"(B) IDENTITY MANAGEMENT PLATFORM WAIVER.—The head of an agency shall be in compliance with the requirement under paragraph (1)(D)(i) with respect to implementing a single-sign on trusted identity system or platform other than one developed by the Adminis-

trator of General Services as described under paragraph (1)(D)(i) if the head of the agency—

"(i) without delegation—

"(I) has certified to the Director that the alternative system or platform, including a procured system or platform, conforms with applicable security and privacy requirements of this subchapter and guidance issued by the Director, at least 30 days before use of the system or platform; or

"(II) with regard to a system or platform in use as of the date of enactment of this subsection, the head of the agency provides such certification to the Director within 60 days after the date of enactment of this subsection;

"(ii) has received a written waiver from the Director in response to the request submitted under clause (i); and

"(iii) has submitted the certification described in clause (i) and the waiver described clause (ii) to the appropriate congressional committees and the authorizing committees of the agency.

"(4) DURATION OF CERTIFICATION.—

"(A) IN GENERAL.—A certification and corresponding exemption of an agency under paragraph (3) shall expire on the date that is 4 years after the date on which the head of the agency submits the certification under paragraph (3).

"(B) RENEWAL.—Upon the expiration of a certification of an agency under paragraph (3), the head of the agency may submit an additional certification in accordance with that paragraph.

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

"(A) the responsibility of any agency to ensure compliance with this subchapter for any cloud computing product or service used by the agency; or

"(B) the authority of the head of any agency to make a determination that there is a demonstrable need to include additional security

controls beyond those included in a FedRAMP authorization package for a particular cloud computing product or service.

"(6) RULES OF CONSTRUCTION.—Nothing in this subsection shall be construed—

"(A) to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of this title;

"(B) to affect the standards or process of the National Institute of Standards and Technology;

"(C) to affect the requirement under section 3553(a)(4);

"(D) to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security; or

"(E) to affect the requirements under subchapter III.

"(g) EXCEPTION.—

"(1) NATIONAL SECURITY SYSTEM REQUIREMENTS.—The requirements under subsection (f)(1) shall not apply to—

"(A) a national security system; or

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

"(2) PROHIBITION.—The prohibition under subsection (f)(2) shall not apply to—

"(A) necessary in the interest of national security;

"(B) national security systems; or

"(C) a procured internet of things device described in subsection (f)(2)(B) that the Chief Information Officer of an agency determines is—

"(i) necessary for research purposes;

"(ii) necessary in the interest of national security; or

"(iii) secured using alternative and effective methods appropriate to the function of the internet of things device.".

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by this Act, is further amended—

(1) in subparagraph (C), by striking "and" at the end;

(2) in subparagraph (D), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(E) with respect to any exemption from the requirements of subsection (f)(3) that is effective on the date of submission of the report, includes the number of information systems that have received an exemption from those requirements.".

(c) GUIDANCE FOR IDENTITY MANAGEMENT SYSTEMS USED BY AGENCIES.—Not later than 1 year after the date of enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Director of the National Institute of Standards and Technology, shall issue, and routinely update thereafter, guidance for agencies to implement identity management systems and a single sign-on trusted identity platform as required under section 3554(f)(1)(D)(i) of title 44, United States Code, as amended by this Act, which shall at a minimum, include the following:

(1) Requirements for agencies to routinely certify that such systems are in compliance with this guidance.

(2) Requirements for agencies to routinely verify and certify that information stored on or transiting through a commercially available product (as defined in section 103 of title 41, United States Code) or commercial service (as defined in section 103a of title 41,

United States Code) used to fulfil such requirements is appropriately secured in conformity with subchapter II of chapter 35 of title 44, United States Code.

(3) Address national security concerns and requirements to ensure the protection of sensitive personal records and biometric data of United States persons from malign foreign ownership, control, or influence and fraud actors.

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

(5) Requirements to prevent discrimination in violation of title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.).

(6) A description of the information necessary to be submitted under the exception described in section 3554(f)(3)(B) of title 44, United States Code, as amended by this Act.

(d) GAO EVALUATION OF TECHNICAL CAPABILITY OF IDENTITY MANAGEMENT SYSTEMS AND PLATFORMS.—Not less frequently than every 3 years for the next 6 years, the Comptroller General shall submit to the appropriate congressional committees a report on whether the single sign-on trusted identity systems and platforms used by agencies

or the one developed by the General Services Administration under section 3554(f)(D)(i) of title 44, United States Code, as amended by this Act, adhere to the information security requirements of chapter 35 of title 44, United States Code, guidance issued under subsection (c), and relevant identity management technical standards promulgated by the National Institute of Standards and Technology, as appropriate, including section 504 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7464).

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

(f) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015 UPDATE.—Section 222(3)(B) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521(3)(B)) is amended by inserting "and the Committee on Oversight and Accountability" before "of the House of Representatives".

SEC. 12. FEDERAL CHIEF INFORMATION SECURITY OFFICER.

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

"§ 3617. Federal Chief Information Security Officer

"(a) ESTABLISHMENT.—There is established a Federal Chief Information Security Officer, who shall serve in—

"(1) the Office of the Federal Chief Information Officer of the Office of Management and Budget; and

"(2) the Office of the National Cyber Director.

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

"(c) OMB DUTIES.—The Federal Chief Information Security Officer shall report to the Federal Chief Information Officer and assist the Federal Chief Information Officer in carrying out—

"(1) every function under this chapter;

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

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

"(4) other Federal cybersecurity initiatives determined by the Federal Chief Information Officer.

"(d) ADDITIONAL DUTIES.—The Federal Chief Information Security Officer shall—

"(1) support the Federal Chief Information Officer in overseeing and implementing Federal cybersecurity under the E–Government Act of 2002 (Public Law 107–347; 116 Stat. 2899) and other relevant statutes in a manner consistent with law; and

"(2) perform every function assigned to the Director under sections 1321 through 1328 of title 41, United States Code.

"(e) COORDINATION WITH ONCD.—The Federal Chief Information Security Officer shall support initiatives determined by the Federal Chief Information Officer necessary to coordinate with the Office of the National Cyber Director.".

(b) NATIONAL CYBER DIRECTOR DUTIES.—Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500) is amended—

(1) by redesignating subsection (g) as subsection (h); and

(2) by inserting after subsection (f) the following:

"(g) SENIOR FEDERAL CYBERSECURITY OFFICER.—The Federal Chief Information Security Officer appointed by the President under section 3617 of title 44, United States Code, shall be a senior official within the Office and carry out duties applicable to the protection of information technology (as defined in section 11101 of title 40, United States Code), including initiatives determined by the Director necessary to coordinate with the Office of the Federal Chief Information Officer.".

(c) TREATMENT OF INCUMBENT.—The individual serving as the Federal Chief Information Security Officer appointed by the President as of the date of enactment of this Act may serve as the Federal Chief Information Security Officer under section 3617 of title 44, United States Code, as added by this Act, beginning on the date of enactment of this Act, without need for a further or additional appointment under such section.

(d) CLERICAL AMENDMENT.—The table of sections for chapter 36 of title 44, United States Code, is amended by adding at the end the following:

"3617. Federal Chief Information Security Officer.".

SEC. 13. RENAMING OFFICE OF THE FEDERAL CHIEF INFORMATION OFFICER.

(a) DEFINITIONS.—

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

(A) by striking paragraph (1); and

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

(2) CONFORMING AMENDMENTS.—

(A) TITLE 10.—Section 2222(i)(6) of title 10, United States Code, is amended by striking "section 3601(4)" and inserting "section 3601".

(B) NATIONAL SECURITY ACT OF 1947.—Section 506D(k)(1) of the National Security Act of 1947 (50 U.S.C. 3100(k)(1)) is amended by striking "section 3601(4)" and inserting "section 3601".

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

*(1) in the heading, by striking "**Office of Electronic Government**" and inserting "**Office of the Federal Chief Information Officer**";*

(2) in subsection (a), by striking "Office of Electronic Government" and inserting "Office of the Federal Chief Information Officer";

(3) in subsection (b), by striking "an Administrator" and inserting "a Federal Chief Information Officer";

(4) in subsection (c), in the matter preceding paragraph (1), by striking "The Administrator" and inserting "The Federal Chief Information Officer";

(5) in subsection (d), in the matter preceding paragraph (1), by striking "The Administrator" and inserting "The Federal Chief Information Officer";

(6) in subsection (e), in the matter preceding paragraph (1), by striking "The Administrator" and inserting "The Federal Chief Information Officer";

(7) in subsection (f)—

(A) in the matter preceding paragraph (1), by striking "the Administrator" and inserting "the Federal Chief Information Officer";

(B) in paragraph (16), by striking "the Office of Electronic Government" and inserting "the Office of the Federal Chief Information Officer"; and

(C) in paragraph (17), by striking "E–Government" and inserting "annual"; and

(8) in subsection (g), by striking "the Office of Electronic Government" and inserting "the Office of the Federal Chief Information Officer".

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

(1) in subsection (b)(2), by striking "The Administrator of the Office of Electronic Government" and inserting "The Federal Chief Information Officer";

(2) in subsection (c)(1), by striking "The Administrator of the Office of Electronic Government" and inserting "The Federal Chief Information Officer"; and

(3) in subsection (f)—

(A) in paragraph (3), by striking "the Administrator" and inserting "the Federal Chief Information Officer"; and

(B) in paragraph (5), by striking "the Administrator" and inserting "the Federal Chief Information Officer".

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

(1) in subsection (a)(2), by striking "the Administrator of the Office of Electronic Government" and inserting "the Federal Chief Information Officer";

(2) in subsection (b), by striking "Administrator" each place it appears and inserting "Federal Chief Information Officer"; and

(3) in subsection (c), in the matter preceding paragraph (1), by striking "the Administrator" and inserting "the Federal Chief Information Officer".

(e) PROGRAM TO ENCOURAGE INNOVATIVE SOLUTIONS TO ENHANCE ELECTRONIC GOVERNMENT SERVICES AND PROCESSES.—Section 3605 of title 44, United States Code, is amended—

(1) in subsection (a), by striking "The Administrator" and inserting "The Federal Chief Information Officer";

(2) in subsection (b), by striking ", the Administrator," and inserting ", the Federal Chief Information Officer,"; and

(3) in subsection (c)—

(A) in paragraph (1)—

(i) by striking "The Administrator" and inserting "The Federal Chief Information Officer"; and

(ii) by striking "proposals submitted to the Administrator" and inserting "proposals submitted to the Federal Chief Information Officer";

(B) in paragraph (2)(B), by striking "the Administrator" and inserting "the Federal Chief Information Officer"; and

(C) in paragraph (4), by striking "the Administrator" and inserting "the Federal Chief Information Officer".

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

*(1) in the section heading by striking "**E–Government**" and inserting "**Annual**";*

(2) in subsection (a), by striking "E–Government" and inserting "annual"; and

(3) in subsection (b)(1), by striking "202(f)" and inserting "202(g)".

(g) TREATMENT OF INCUMBENT.—The individual serving as the Administrator of the Office of Electronic Government under section 3602 of title 44, United States Code, as of the date of enactment of this Act, may continue to serve as the Federal Chief Information Officer commencing as of that date, without need for a further or additional appointment under such section.

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

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

"3602. Office of the Federal Chief Information Officer.";

and

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

(i) REFERENCES.—

(1) ADMINISTRATOR.—Any reference to the Administrator of the Office of Electronic Government in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Federal Chief Information Officer.

(2) OFFICE OF ELECTRONIC GOVERNMENT.—Any reference to the Office of Electronic Government in

any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Office of the Federal Chief Information Officer.

SEC. 14. RULES OF CONSTRUCTION.

(a) AGENCY ACTIONS.—Nothing in this Act, or an amendment made by this Act, shall be construed to authorize the head of an agency to take an action that is not authorized by this Act, an amendment made by this Act, or existing law.

(b) PROTECTION OF RIGHTS.—Nothing in this Act, or an amendment made by this Act, shall be construed to permit the violation of the rights of any individual protected by the Constitution of the United States, including through censorship of speech protected by the Constitution of the United States or unauthorized surveillance.

(c) PROTECTION OF PRIVACY.—Nothing in this Act, or any amendment made by this Act, shall be construed to—

(1) impinge on the privacy rights of individuals; or

(2) allow the unauthorized access, sharing, or use of personal data.

Union Calendar No. 790

118TH CONGRESS
2D SESSION

H. R. 4552

[Report No. 118–939, Part I]

A BILL

To improve the cybersecurity of the Federal Government, and for other purposes.

DECEMBER 19, 2024

Reported from the Committee on Oversight and Accountability with an amendment

DECEMBER 19, 2024

Committees on Science, Space, and Technology, Homeland Security, and Armed Services discharged; committed to the Committee of the Whole House on the State of the Union and ordered to be printed