notification entities a report on the activities of the Task Force, including—

(i) recommendations on—

(I) priorities for research and development in the systems that enable digital identity verification, including how the priorities can be executed;

(II) the standards-based architecture developed pursuant to paragraph (7)(D);

(III) methods to leverage digital driver's licenses, distributed ledger technology, and other technologies; and

(IV) priorities for research and development in the systems and processes that reduce identity fraud; and

(ii) summaries of the input and recommendations of the leaders consulted under paragraph (9).

(B) INTERIM REPORTS.—

(i) IN GENERAL.—The Director may submit to the appropriate notification entities interim reports the Director determines necessary to support the work of the Task Force and educate the public.

(ii) MANDATORY REPORT.—Not later than the date that is 18 months after the date of enactment of this Act, the Director shall submit to the appropriate notification entities an interim report addressing—

(I) the matters described in subparagraphs (A), (B), (D), and (F) of paragraph (7); and

(II) any other matters the Director determines necessary to support the work of the Task Force and educate the public.

(C) FINAL REPORT.—Not later than 180 days before the date described in paragraph (11), the Director shall submit to the appropriate notification entities a final report that includes recommendations for the President and Congress relating to any relevant matter within the scope of the duties of the Task Force.

(D) PUBLIC AVAILABILITY.—The Task Force shall make the reports required under this paragraph publicly available on centralized website as an open Government data asset (as defined in section 3502 of title 44, United States Code).

(11) SUNSET.—The Task Force shall conclude business on the date that is 3 years after the date of enactment of this Act.

(d) SECURITY ENHANCEMENTS TO FEDERAL SYSTEMS.—

(1) GUIDANCE FOR FEDERAL AGENCIES.—Not later than 180 days after the date on which the Director submits the report required under subsection (c)(10)(A), the Director of the Office of Management and Budget shall issue guidance to Federal agencies for the purpose of implementing any recommendations included in such report determined appropriate by the Director of the Office of Management and Budget.

(2) REPORTS ON FEDERAL AGENCY PROGRESS IMPROVING DIGITAL IDENTITY VERIFICATION CAPABILITIES.—

(A) ANNUAL REPORT ON GUIDANCE IMPLEMENTATION.—Not later than 1 year after the date of the issuance of guidance under paragraph (1), and annually thereafter, the head of each Federal agency shall submit to the Director of the Office of Management and Budget a report on the efforts of the Federal agency to implement that guidance.

(B) PUBLIC REPORT.—

(i) IN GENERAL.—Not later than 45 days after the date of the issuance of guidance under paragraph (1), and annually thereafter, the Director shall develop and make publicly available a report that includes—

(I) a list of digital identity verification services offered by Federal agencies;

(II) the volume of digital identity verifications performed by each Federal agency;

(III) information relating to the effectiveness of digital identity verification services by Federal agencies; and

(IV) recommendations to improve the effectiveness of digital identity verification services by Federal agencies.

(ii) CONSULTATION.—In developing the first report required under clause (i), the Director shall consult the Task Force.

(C) CONGRESSIONAL REPORT ON FEDERAL AGENCY DIGITAL IDENTITY CAPABILITIES.—

(i) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report relating to the implementation and effectiveness of the digital identity capabilities of Federal agencies.

(ii) CONSULTATION.—In developing the report required under clause (i), the Director of the Office of Management and Budget shall—

(I) consult with the Task Force; and

(II) to the greatest extent practicable, include in the report recommendations of the Task Force.

(iii) CONTENTS OF REPORT.—The report required under clause (i) shall include—

(I) an analysis, including metrics and milestones, for the implementation by Federal agencies of—

(aa) the guidelines published by the National Institute of Standards and Technology in the document entitled ''Special Publication 800–63'' (commonly referred to as the ''Digital Identity Guidelines''), or any successor document; and

(bb) if feasible, any additional requirements relating to enhancing digital identity capabilities identified in the document of the Office of Management and Budget entitled ''M–19–17'' and issued on May 21, 2019, or any successor document;

(II) a review of measures taken to advance the equity, accessibility, cybersecurity, and privacy of digital identity verification services offered by Federal agencies; and

(III) any other relevant data, information, or plans for Federal agencies to improve the digital identity capabilities of Federal agencies.

(3) ADDITIONAL REPORTS.—On the first March 1 occurring after the date described in paragraph (2)(C)(i), and annually thereafter, the Director of the Office of Management and Budget shall include in the report required under section 3553(c) of title 44, United States Code—

(A) any additional and ongoing reporting on the matters described in paragraph (2)(C)(iii); and

(B) associated information collection mechanisms.

(e) GAO REPORT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the estimated potential savings, including estimated annual potential savings, due to the increased adoption and widespread use of digital identification, of—

(A) the Federal Government from averted fraud, including benefit fraud; and

(B) the economy of the United States and consumers from averted identity theft .

(2) CONTENTS.—Among other variables the Comptroller General of the United States determines relevant, the report required under paragraph (1) shall include multiple scenarios with varying uptake rates to demonstrate a range of possible outcomes.

SA 5815. Mr. PETERS (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

DIVISION ____—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2022

SEC. ___01. SHORT TITLE.

This division may be cited as the ''Federal Information Security Modernization Act of 2022''.

SEC. ___02. DEFINITIONS.

In this division, unless otherwise specified:

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

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

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

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

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

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

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

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

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

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

(8) 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.

(9) 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. ___03. 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) confidentiality, privacy, 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), 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, and 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 coordinate, as appropriate, with the Chief Data Officer in accordance with the designated functions under section 3520(c).'' after ''reduction of information collection burdens on the public.'';

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

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

(4) in section 3513—

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

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

''(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security to the 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 (1), (2), (3), (4), (5), (6), and (7) as paragraphs (2), (4), (5), (6), (7), (9), and (11), respectively;

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

''(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.'';

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

''(3) The term 'high value asset' means information or an information system that the head of an agency, using policies, principles, standards, or guidelines issued by the Director under section 3553(a), in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, determines to be so critical to the agency that the loss or degradation of the confidentiality, integrity, or accessibility 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.'';

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

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

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

''(10) The term 'penetration test'—

''(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 (11), as so redesignated, the following:

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

''(13) 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(1)(A)) is amended by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''.

(B) TITLE 10.—

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

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

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

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

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

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

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

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

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

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

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

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

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

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

(ii) in subsection (f)—

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

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

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

(1) in section 3551—

(A) 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 (1), by inserting '', in consultation with the Secretary and the National Cyber Director,'' before ''overseeing'';

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

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

(iv) by adding at the end the following:

''(8) 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 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 a classified annex,'' 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;

(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

(vi) in paragraph (5), by striking the period at the end and inserting ''; 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''; and

(II) 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 continuous 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 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); and

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

(F) by adding at the end the following:

''(m) BINDING OPERATIONAL DIRECTIVES.—If the Secretary issues a binding operational directive or an emergency directive under this section, not later than 4 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Director, National Cyber Director, the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives the status of the implementation of the binding operational directive at the agency.

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

''(1) CONDUCT OF REVIEW.—The Director of the Office of Management and Budget shall regularly review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including 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 Reform of the House of Representatives of planned changes to guidance or policy resulting from the review in paragraph (1).

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

''(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, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, 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 (i) to the Council of the Inspectors General on Integrity and Efficiency.'';

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

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

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

''(A) on an ongoing and continuous basis, assessing agency system risk 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 agency systems that have access to or hold the data assets inventoried under section 3511;

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

''(v) 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;

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

''(vii) 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; and

(V) by adding at the end the following:

''(E) providing an update on the ongoing and continuous 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) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

''(I) the Director;

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

''(III) the National Cyber Director;

''(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

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

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

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

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

''(ii) the Director; and

''(iii) the National Cyber Director; and

''(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency;'';

(ii) in paragraph (2)—

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

(II) in subparagraph (B)—

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

''(i) standards''; and

(bb) by adding at the end the following:

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

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

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

(iii) in paragraph (3)—

(I) in subparagraph (A)—

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

(bb) in clause (iv), by adding ''and'' at the end; and

(cc) by adding at the end the following:

''(v) ensure that—

''(I) senior agency information security officers of component agencies carry out responsibilities under this subchapter, as directed by the senior agency information security officer of the agency or an equivalent official; and

''(II) senior agency information security officers of component agencies report to—

''(aa) the senior information security officer of the agency or an equivalent official; and

''(bb) the Chief Information Officer of the component agency or an equivalent official;''; and

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

(B) in subsection (b)—

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

''(1) the ongoing and continuous 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) and inserting the following:

''(B) comply with the risk-based budget model developed pursuant to section 3553(a)(7);''; and

(II) in subparagraph (D)—

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

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

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

(cc) in clause (iv), as so redesignated, by striking ''as determined by the agency; and'' and inserting ''as determined by the agency, considering 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 providing the status of every remedial action and unremediated identified system vulnerability to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;''; and

(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);

(C) in subsection (c)—

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

(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 2022 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment required under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

''(A) summarizes the agency system risk assessment 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 evaluation and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether those evaluation and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency; and

''(D) summarizes the status of remedial actions identified by inspector general of the agency, the Comptroller General of the United States, and any other source determined appropriate by the head of the agency.

''(2) UNCLASSIFIED REPORTS.—Each report submitted under paragraph (1)—

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

''(B) may include a classified annex.

''(3) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified form of the report submitted by the agency under paragraph (2)(A).

''(4) BRIEFINGS.—During each year during which a report is not required to be submitted under paragraph (1), the Director shall provide to the congressional committees described in paragraph (1) a briefing summarizing current agency and Federal risk postures.''; and

(iii) in paragraph (5), as so redesignated, by 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'';

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting ''and the National Cyber Director'' after ''the Director''; and

(E) by adding at the end the following:

''(f) REPORTING STRUCTURE EXEMPTION.—

''(1) IN GENERAL.—On an annual basis, the Director may exempt an agency from the reporting structure requirement under subsection (a)(3)(A)(v)(II).

''(2) REPORT.—On an annual basis, the Director shall submit a report to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives that includes a list of each exemption granted under paragraph (1) and the associated rationale for each exemption.

''(3) COMPONENT OF OTHER REPORT.—The report required under paragraph (2) may be incorporated into any other annual report required under this chapter.'';

(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).''; and

(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 experienced by each agency;

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

''(C) any other security risks unique to the networks of each agency; and

''(D) any other element the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Council of the Inspectors General on Integrity and Efficiency, determines appropriate.''; 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 submitted under section 3553(c) of title 44, United States Code''; and

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

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

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

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

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

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

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''§ 3591. Definitions

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

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

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

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

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

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

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

''(E) the Committee on Oversight and Reform 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) a contractor of an agency;

''(ii) the recipient of a grant from an agency;

''(iii) a party to a cooperative agreement with an agency; and

''(iv) a party to an other transaction agreement with an agency; and

''(B) includes a subgrantee 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 or any similar occurrence; and

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

''(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.

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

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

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

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

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

''§ 3592. Notification of breach

''(a) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with the senior privacy officer of the agency, shall—

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

''(A) the nature and sensitivity of the personally identifiable information affected by the breach;

''(B) the likelihood of access to and use of the personally identifiable information affected by the breach;

''(C) the type of breach; and

''(D) any other factors determined by the Director; and

''(2) as appropriate, provide written notice in accordance with subsection (b) to each individual potentially affected by the breach—

''(A) to the last known mailing address of the individual; or

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

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

''(1) a brief description of the breach;

''(2) if possible, a description of the types of personally identifiable information affected by the breach;

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

''(A) shall include an e-mail address or another digital contact mechanism; and

''(B) may include a telephone number, mailing address, or a website;

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

''(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identifiable information, including relevant contact information for Federal law enforcement agencies and each nationwide consumer reporting agency; and

''(6) any other appropriate information, as determined by the head of the agency or established in guidance by the Director.

''(c) DELAY OF NOTIFICATION.—

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

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

''(B) reveal sensitive sources and methods;

''(C) cause damage to national security; or

''(D) hamper security remediation actions.

''(2) DOCUMENTATION.—

''(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the Director, the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

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

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

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

''(d) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (a)(1), or that it is necessary to update the details of the information provided to potentially affected individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

''(e) DELAY AND LACK OF NOTIFICATION REPORT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Federal Information Security Modernization Act of 2022, and annually thereafter, an official who delays a notification under subsection (c) shall submit to the appropriate reporting entities a report on the delay.

''(2) LACK OF BREACH NOTIFICATION.—The Director shall submit to the appropriate reporting entities an annual report on each breach with respect to which the head of an agency determined, pursuant to subsection (a)(1), not to notify individuals potentially impacted by the breach.

''(3) COMPONENT OF OTHER REPORT.—The Director may submit the report required under paragraph (1) as a component of the annual report submitted under section 3597(b).

''(f) CONGRESSIONAL REPORTING REQUIREMENTS.—

''(1) IN GENERAL.—On a periodic basis, the Director of the Office of Management and Budget shall update 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 breach to expeditiously and not later than 30 days after the date on which the agency discovers the breach give notice of the breach 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 breach provided by the head of an agency pursuant to paragraph (2) shall include—

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

''(B) an estimate of the number of individuals affected by the 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 breach; and

''(D) an estimate of whether and when the agency will provide notice to individuals affected by the breach.

''(4) EXCEPTION.—An element of the intelligence community that is required to provide notice pursuant to paragraph (2) shall only provide such notice to the appropriate committees of Congress.

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

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

''(1) the authority of the Director from issuing guidance relating to notifications of, or the head of an agency from notifying individuals potentially affected by, breaches that are not determined to be major incidents;

''(2) the authority of the Director from issuing guidance relating to notifications of major incidents;

''(3) the authority of the head of an agency from providing more information than required under subsection (b) when notifying individuals potentially affected by a breach; or

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

''(A) the Director;

''(B) the National Cyber Director;

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

''(D) any other agency.

''§ 3593. Congressional and Executive Branch reports

''(a) INITIAL REPORT.—

''(1) IN GENERAL.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entities a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Science, Space, and Technology of the House of Representatives, and the appropriate authorization and appropriations committees of Congress.

''(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner consistent with section 552a of title 5, United States Code—

''(A) a summary of the information available about the major incident, including how the major incident occurred and, if applicable information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

''(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in a notification to individuals potentially affected by the major incident under section 3592(c);

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

''(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; and

''(E) information available about the major incident, taking into account—

''(i) the information known at the time of the report;

''(ii) the sensitivity of the details associated with the major incident; and

''(iii) the classification level of the information contained in the report.

''(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 30 days after the date on which an agency submits a written report under subsection (a), the head of the agency shall provide to the appropriate reporting entities written updates, which may include classified annexes, on the major incident and, to the extent practicable, provide a briefing, which may include a classified component, to the congressional committees described in subsection (a)(1), including summaries of—

''(1) vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

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

''(3) the status of compliance of the affected information system with applicable security requirements, including the requirements of section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523), at the time of the major incident;

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

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

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

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

''(8) if applicable, a description of any data or circumstances leading the head of the agency to determine, pursuant to section 3592(a)(1), not to notify individuals potentially impacted by a breach.

''(c) UPDATE REPORT.—If the 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 an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

''(d) 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.

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

''(f) THREAT BRIEFING.—

''(1) IN GENERAL.—Not later than 7 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the impacted agency shall coordinate with the National Cyber Director and consult with the Director and any other Federal entity determined appropriate by the National Cyber Director to provide a briefing to the congressional committees described in subsection (a)(1) on the threat causing the major incident.

''(2) COMPONENTS.—The briefing required under paragraph (1)—

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

''(B) may include a classified component.

''(g) REPORT AND BRIEFING 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 and briefings required under this section, including recommendations for consistent formats for presenting any associated metrics; and

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

''(A) include, at a minimum—

''(i) the full contents of the report;

''(ii) the reporting agency; and

''(iii) the date of submission; and a list of the recipient congressional entities; and

''(B) be made available upon request to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives.

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

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

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

''§ 3594. Government information sharing and incident response

''(a) IN GENERAL.—

''(1) INCIDENT REPORTING.—Subject to the limitations described in subsection (b), the head of each agency shall provide to the Cybersecurity 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, at a minimum—

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

''(B) identify whether the agency implemented the safeguards described in subparagraph (A) correctly;

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

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

''(ii) additional necessary safeguards; and

''(D) include information to aid in incident response, such as—

''(i) a description of the affected systems or networks;

''(ii) the estimated dates of when the incident occurred; and

''(iii) information that could reasonably help identify the party that conducted the incident or the cause of 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) similarly 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.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

''(b) COMPLIANCE.—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 enables automated and consistent reporting 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, regardless of delays from notification granted for a major incident that is also a breach, 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) REPORTING.—

''(1) IN GENERAL.—With respect to the agency with which an awardee has a contract, grant, cooperative agreement, or other transaction agreement, within the same amount of time that agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency under section 3594(a), the awardee shall report to the head of that agency and the Director of the Cybersecurity and Infrastructure Security Agency if the awardee has a reasonable basis to suspect or conclude that—

''(A) an incident or breach has occurred with respect to Federal information collected, used, or maintained by the awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement;

''(B) an incident or breach has occurred with respect to a Federal information system used or operated by the awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement; or

''(C) the awardee has received information from the agency that the awardee is not authorized to receive in connection with the contract, grant, cooperative agreement, or other transaction agreement.

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

''(b) REGULATIONS; MODIFICATIONS.—Not later than 1 year after the date of enactment of the Federal Information Security Modernization Act of 2022, the head of each agency shall—

''(1) promulgate regulations, policies, and procedures, as appropriate, relating to the responsibilities of awardees to comply with this section; and

''(2) modify each existing contract, grant, cooperative agreement, and other transaction agreement of the agency to comply with this section.

''§ 3596. Training

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

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

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

''(b) GUIDANCE.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology, shall develop guidance containing minimum standards for 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, including the information to be collected and a requirement that such information be reported in a machine-readable format to the greatest extent practicable;

''(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; and

''(3) appropriate training and qualification standards for information technology personnel and cyber incident responders.

''(c) TRAINING.—The head of each agency shall develop training for covered individuals that adheres to the guidance developed under subsection (b).

''(d) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (c) may be included as part of an annual privacy or security awareness training of an agency.

''§ 3597. Analysis and report on Federal incidents

''(a) ANALYSIS OF FEDERAL INCIDENTS.—

''(1) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency shall perform and, in consultation with the Director and the National Cyber Director, develop, continuous monitoring and quantitative and qualitative analyses of incidents at agencies, including major incidents, including—

''(A) the causes of incidents, including—

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

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

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

''(C) 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 extent 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 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.

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

''(2) EXEMPTION.—The Director of the Cybersecurity and Infrastructure Security Agency shall exempt all or a portion of a report described in paragraph (1) from public publication if the Director of the Cybersecurity and Infrastructure Security Agency or the National Cyber Director determines the exemption is in the interest of national security.

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

''(d) INFORMATION PROVIDED BY AGENCIES.—

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

''(2) NONCOMPLIANCE REPORTS.—

''(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes the information described in subsection (b) with respect to the agency.

''(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

''(3) NATIONAL SECURITY SYSTEM REPORTS.—

''(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the national security system to the extent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

''(i) the majority and minority leaders of the Senate,

''(ii) the Speaker and minority leader of the House of Representatives;

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

''(iv) the Select Committee on Intelligence of the Senate;

''(v) the Committee on Armed Services of the Senate;

''(vi) the Committee on Appropriations of the Senate;

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

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

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

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

''(xi) the Committee on Appropriations of the House of Representatives.

''(B) CLASSIFIED FORM.—A report required under subparagraph (A) may be submitted in a classified form.

''(e) REQUIREMENT FOR COMPILING INFORMATION.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director and the National Cyber Director, and in consultation with the impacted agency.

''§ 3598. Major incident definition

''(a) IN GENERAL.—Not later than 1 year after the date of enactment of the Federal Information Security Modernization Act of 2022, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

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

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

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

''(i) the national security, 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 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;

''(3) stipulate that the National Cyber Director, in consultation with the Director and the Director of the Cybersecurity and Infrastructure Security Agency, shall consider declaring a major incident at any agency impacted by an incident if it is determined that an incident—

''(A) occurs at not less than 2 agencies; and

''(B) is enabled by—

''(i) a common technical root cause, such as a supply chain compromise, or a common software or hardware vulnerability; or

''(ii) the related activities of a common threat actor;

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

''(5) 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 2 years after the date on which the Director promulgates the guidance required under subsection (a), and not less frequently than every 2 years thereafter, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing 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

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

SEC. ___04. 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 to be reviewed by the member of the Technology Modernization Board described in subsection (c)(5)(C)—

''(i) a cybersecurity risk management plan; and

''(ii) a supply chain risk management plan.''; 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,'';

(B) in subsection (c)(3)—

(i) in subparagraph (A)—

(I) by striking ''including data'' and inserting ''which shall—

''(i) include data''; and

(II) by adding at the end the following:

''(ii) specifically denote cybersecurity funding under the risk-based budget model developed pursuant to section 3553(a)(7) of title 44.''; and

(ii) in subparagraph (B), by adding at the end the following:

''(iii) The Director shall provide to the National Cyber Director any cybersecurity funding information described in subparagraph (A)(ii) that is provided to the Director under clause (ii) of this subparagraph.''; and

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

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

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

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

(iii) by adding at the end the following:

``(iii) whether the function should be performed by a shared service offered by another executive agency;''; and

(B) in paragraph (5)(B)(i), by inserting ``, while taking into account the risk-based budget model developed pursuant to section 3553(a)(7) of title 44'' after ``title 31''.

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

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

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

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

``(d) COMPONENT AGENCY CHIEF INFORMATION OFFICERS.—The Chief Information Officer or an equivalent official of a component agency shall report to—

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

``(2) the head of the component agency.

``(e) REPORTING STRUCTURE EXEMPTION.—

``(1) IN GENERAL.—On annual basis, the Director may exempt any agency from the reporting structure requirements under subsection (d).

``(2) REPORT.—On an annual basis, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a report that includes a list of each exemption granted under paragraph (1) and the associated rationale for each exemption.

``(3) COMPONENT OF OTHER REPORT.—The report required under paragraph (2) may be incorporated into any other annual report required under chapter 35 of title 44, United States Code.'';

(4) in section 11317, by inserting ``security,'' before ``or schedule''; and

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

SEC. ____05. 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 of the analysis required under section 3597(a) of title 44, United States Code, as added by this division, 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 division.

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

(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 division;

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

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

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 552a(b)(13) of title 5, United States Code, as added by this section, to provide information to other agencies experiencing incidents.

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

(5) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to 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 division.

(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.

(6) UPDATED BRIEFINGS.—Not later than 30 days after the Director updates guidance or templates under paragraph (2)(A) or (4), the Director shall provide to the appropriate congressional committees a briefing on such updates.

(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, in furtherance of a response to an incident (as defined in section 3552 of title 44) or to fulfill the information sharing requirements under section 3594 of title 44, provided that the disclosing agency maintains documentation specifying the particular portion shared and the activity for which the record is disclosed.''.

SEC. ____06. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

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

(1) performing the ongoing and continuous agency system risk assessment required under section 3554(a)(1)(A) of title 44, United States Code, as amended by this division;

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

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

(A) specific guidance for the use of automation and machine-readable data; and

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

(4) a requirement to coordinate with inspectors general of agencies to ensure consistent understanding and application of agency policies for the purpose of evaluations by inspectors general.

SEC. ____07. 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 issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

(1) the confidentiality or integrity of sensitive information submitted by the reporting entity to the agency pursuant to a statutory or regulatory requirement; or

(2) any agency information system used in the transmission or storage of the sensitive information described in paragraph (1).

SEC. ____08. MOBILE SECURITY STANDARDS.

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

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

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

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

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

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

(2) a requirement for each agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(B) and other risks associated with the use of applications on mobile devices; and

(3) instructions on sharing the inventory of the agency required under paragraph (1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

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

SEC. ___09. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

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

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

(1) the types of logs to be maintained;

(2) the duration that logs and other relevant data should be retained;

(3) the time periods for agency implementation of recommended logging and security requirements;

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

(5) requirements to ensure that, upon request, in a manner consistent section 552a of title 5, United States Code, agencies provide logs to—

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

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

(6) requirements to ensure that the highest level security operations center of each agency has visibility into all agency logs.

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall, as determined to be appropriate by the Director, update guidance to agencies regarding requirements for logging, log retention, log management, sharing of log data with other appropriate agencies, or any other logging activity determined to be appropriate by the Director.

(d) SUNSET.—This section shall cease to have force or effect on the date that is 10 years after the date of the enactment of this Act.

SEC. ___10. CISA AGENCY ADVISORS.

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

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

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

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

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

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

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

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

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

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

(f) COORDINATION OF ACTIVITIES.—The Director of the Cybersecurity and Infrastructure Security Agency shall consult with the Director on the execution of the duties of the Cybersecurity and Infrastructure Security Agency advisors to ensure that there is no inappropriate duplication of activities among—

(1) Federal cybersecurity support to agencies of the Office of Management and Budget; and

(2) the Cybersecurity and Infrastructure Security Agency advisors.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed impact the ability of the Director to support agency implementation of Federal cybersecurity requirements pursuant to subchapter II of chapter 35 of title 44, United States Code, as amended by this Act.

SEC. ___11. 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 use, when and where appropriate, penetration testing by both Federal and non-Federal entities on agency systems with a focus on high value assets;

''(2) provides policies governing the development of—

''(A) an agency operational plan;

''(B) rules of engagement for using penetration testing; and

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

''(3) ensures that—

''(A) penetration testing is performed appropriately by agencies; and

''(B) 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 of title 44, United States Code, 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) DEADLINE FOR GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall issue the guidance required under section 3559A(a) of title 44, United States Code, as added by subsection (a).

(c) 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) SUNSET.—

(1) IN GENERAL.—Effective on the date that is 10 years after the date of enactment of this Act, subchapter II of chapter 35 of title 44, United States Code, is amended by striking section 3559A.

(2) CLERICAL AMENDMENT.—Effective on the date that is 10 years after the date of enactment of this Act, the table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3559A.

(e) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by section ___03, is further amended by inserting after paragraph (8) the following:

''(9) performing penetration testing to identify vulnerabilities within Federal information systems;''.

SEC. ___12. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall establish a program to provide ongoing, proactive threat-hunting services in accordance with authorities granted under section paragraphs (7) and (10) of subsection (b) and subsection (l) of section 3553 of title 44,United States Code, as amended by this Act, which may be offered as a shared service, on the networks of each agency.

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

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

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

(D) establish common operating procedures, including necessary interagency legal agreements;

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

(F) provide input to the heads of agencies on the use of additional cybersecurity procedures under section 3554 of title 44, United States Code.

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

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

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program under subsection (a)(1), a report providing any updates to the plan developed under subsection (a)(2); and

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

SEC. ___13. VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section ___11 of this division, the following:

''§ 3559B. Federal vulnerability disclosure programs

''(a) PURPOSE; SENSE OF CONGRESS.—

''(1) PURPOSE.—The purpose of Federal vulnerability disclosure programs is to create a mechanism to use the expertise of the public to provide a service to agencies by identifying information system vulnerabilities.

''(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) 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).

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

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

''(c) RESPONSIBILITIES OF OMB.—

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

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

''(B) is otherwise authorized under the vulnerability disclosure policy of the agency developed under subsection (e)(2).

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

''(A) any valid or credible vulnerability disclosure reports of newly discovered or not publicly known security vulnerabilities (including misconfigurations) in commercial software or services used by Federal information systems;

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

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

''(ii) about which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency should know; and

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

''(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—

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

''(B) LIMITATION.—The guidance to agencies under subparagraph (A) shall stipulate 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.

''(d) 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.

''(e) RESPONSIBILITIES OF AGENCIES.—

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

''(A) an appropriate security contact; and

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

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

''(A) describe—

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

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

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

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

''(B) with respect to a 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 Federal 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 under paragraph (2); and

''(B) commensurate with the risk posed by the security vulnerability, address such security vulnerability using the security vulnerability management process of the agency.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2022, and annually thereafter for a 3-year period, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the heads of impacted agencies, shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (c)(3), an identification of the agencies that are compliant and not compliant.

''(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infrastructure Security Agency under this section shall not apply to national security systems.

''(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director and the Director of the Cybersecurity and Infrastructure Security Agency described in this section shall be delegated—

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

''(2) to the Director of National Intelligence in the case of systems described in section 3553(e)(3).''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559A, as added by section ___11 of this division, the following:

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

(c) SUNSET.—

(1) IN GENERAL.—Effective on the date that is 10 years after the date of enactment of this Act, subchapter II of chapter 35 of title 44, United States Code, is amended by striking section 3559B.

(2) CLERICAL AMENDMENT.—Effective on the date that is 10 years after the date of enactment of this Act, the table of sections for chapter 35 of title 44, United States Code, is amended by striking the item relating to section 3559B.

SEC. ___14. IMPLEMENTING ZERO TRUST ARCHITECTURE.

(a) REPORT.—Not later than 18 months 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 Reform and Homeland Security of the House of Representatives an update 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;

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

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

(b) PROGRESS REPORT.—As a part of the report required under section 3553(c) of title 44, United States Code, the Director shall include an update on agency implementation of information security programs based on the presumption of compromise and least privilege, such as 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.—The update required under subsection (b) may include a classified annex, as appropriate.

SEC. ___15. GAO AUTOMATION REPORTS.

Not later than 2 years after the date of the enactment of this Act, the Comptroller General of the United States shall perform a study, and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Reform and Homeland Security of the House of Representatives a report, on the use of automation and machine-readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes employed by agencies under paragraphs (1), (5)(C), and (8)(B) of section 3554(b) of title 44, United States Code, as amended by this Act.

SEC. ___16. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL AND SOFTWARE INVENTORY.

(a) EXTENSION.—Section 1328 of title 41, United States Code, is amended by striking ''the date that'' and all that follows and inserting ''December 31, 2028.''.

(b) EXTENSION.—Section 4713(j) of title 41, United States Code, is amended by striking ''the date that'' and all that follows and inserting ''December 31, 2028.''.

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

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

(2) by redesignating paragraph (6) as paragraph (7); and

(3) by inserting after paragraph (5) the following:

''(6) maintaining an up-to-date and accurate inventory of software in use by the agency and, when available and applicable, the components of such software, including any available software bills of materials, as applicable, that will be provided within 30 days of receiving a request from the Federal Acquisition Security Council, the individual serving as the Administrator of the Office of Electronic Government, the National Cyber Director, or the Director of Cybersecurity and Infrastructure Security Agency; and''.

SEC. ___17. EXTENSION OF CHIEF DATA OFFICER COUNCIL.

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

SEC. ___18. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) in paragraph (2)—

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

(B) by redesignating subparagraph (B) as subparagraph (C);

(C) by inserting after subparagraph (A) the following:

''(B) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44, United States Code; and''; and

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

''(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to require the publication of information that is exempted from disclosure under section 552 of title 5, United States Code''.

SEC. ___19. QUANTITATIVE CYBERSECURITY METRICS.

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

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

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

(2) as appropriate and pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)) update or establish new covered metrics.

(c) IMPLEMENTATION.—

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

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

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

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

(5) TIME-BASED METRIC.—With respect the first update or establishment of covered metrics required under subsection (b)(2), the Director of the Cybersecurity and Infrastructure Security Agency shall establish covered metrics that include not less than 2 metrics addressing the time it takes for agencies to identify and respond to incidents.

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

(e) 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 Reform'' before ''of the House of Representatives.''

SEC. ___20. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) DEFINITIONS.—In this section:

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

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

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

(2) COVERED AGENCY.—The term ''covered agency'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code.

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

(4) INFORMATION TECHNOLOGY.—The term ''information technology''—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

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

(5) RISK-BASED BUDGET.—The term ''risk-based budget'' means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

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

(1) IN GENERAL.—

(A) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Director of the National Institute of Standards and Technology, shall develop a standard model for informing a risk-based budget for cybersecurity spending.

(B) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section ___03 of this division, is further amended by inserting after paragraph (6) the following:

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

(C) CONTENTS OF MODEL.—The model required to be developed under subparagraph (A) shall utilize appropriate information to evaluate risk, including, as determined appropriate by the Director—

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

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

(iii) to the greatest extent practicable, analysis of where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities.

(D) USE OF MODEL.—The model required to be developed under subparagraph (A) shall be used to—

(i) inform acquisition and sustainment of—

(I) information technology and cybersecurity tools;

(II) information technology and cybersecurity architectures;

(III) information technology and cybersecurity personnel; and

(IV) cybersecurity and information technology concepts of operations; and

(ii) evaluate and inform Government-wide cybersecurity programs.

(E) MODEL VARIATION.—The Director may develop multiple models under subparagraph (A) based on different agency characteristics, such as size or cybersecurity maturity.

(F) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under subparagraph (A).

(G) PUBLICATION.—Not earlier than 5 years after the date on which the model developed under subparagraph (A) is completed, the Director shall, taking into account any classified or sensitive information, publish the model, and any updates necessary under subparagraph (F), on the public website of the Office of Management and Budget.

(H) REPORTS.—Not later than 2 years after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under subparagraph (A) is completed, whichever is sooner, the Director shall submit to the appropriate congressional committees a report on the development of the model.

(2) PHASED IMPLEMENTATION OF RISK-BASED BUDGET MODEL.—

(A) INITIAL PHASE.—

(i) IN GENERAL.—Not later than 2 years after the date on which the model developed under paragraph (1) is completed, the Director shall require not less than 5 covered agencies to use the model to inform the development of the annual cybersecurity and information technology budget requests of those covered agencies.

(ii) BRIEFING.—Not later than 1 year after the date on which the covered agencies selected under clause (i) begin using the model developed under paragraph (1), the Director shall provide to the appropriate congressional committees a briefing on implementation of risk-based budgeting for cybersecurity spending, an assessment of agency implementation, and an evaluation of whether the risk-based budget helps to mitigate cybersecurity vulnerabilities.

(B) FULL DEPLOYMENT.—Not later than 5 years after the date on which the model developed under paragraph (1) is completed, the head of each covered agency shall use the model, or any updated model pursuant to paragraph (1)(F), to the greatest extent practicable, to inform the development of the annual cybersecurity and information technology budget requests of the covered agency.

(C) AGENCY PERFORMANCE PLANS.—

(i) AMENDMENT.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ''and the risk-based budget model required under section 3553(a)(7)'' after ''paragraph (1)''.

(ii) EFFECTIVE DATE.—The amendment made by clause (i) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(3) VERIFICATION.—

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

(i) in the matter preceding subclause (I), by striking ''by agency, and by initiative area (as determined by the administration)'' and inserting ''and by agency'';

(ii) in subclause (III), by striking ''and'' at the end; and

(iii) by adding at the end the following:

''(V) a validation that the budgets submitted were informed by using a risk-based methodology; and

''(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.''.

(B) EFFECTIVE DATE.—The amendments made by subparagraph (A) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(4) REPORTS.—

(A) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

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

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

(iii) by adding at the end the following:

''(D) an assessment of how the agency was informed by the risk-based budget model required under section 3553(a)(7) and an evaluation of whether the model mitigates agency cyber vulnerabilities.''.

(B) ASSESSMENT.—

(i) AMENDMENT.—Section 3553(c) of title 44, United States Code, as amended by section ____03 of this division, is further amended by inserting after paragraph (5) the following:

''(6) an assessment of—

''(A) Federal agency utilization of the model required under subsection (a)(7); and

''(B) whether the model mitigates the cyber vulnerabilities of the Federal Government.''.

(ii) EFFECTIVE DATE.—The amendment made by clause (i) shall take effect on the date that is 5 years after the date on which the model developed under paragraph (1) is completed.

(5) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by paragraph (3), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(A) an evaluation of the success of covered agencies in utilizing the risk-based budget model;

(B) an evaluation of the success of covered agencies in implementing risk-based budgets;

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

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

SEC. ____21. ACTIVE CYBER DEFENSIVE STUDY.

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

(1) has the meaning given the term by the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, the Attorney General, and the heads of other appropriate agencies; and

(2) includes, at a minimum—

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

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

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director and the National Cyber Director, shall perform a study, and submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committees on Oversight and Reform and Homeland Security of the House of Representatives a report, on the use of active defense techniques to enhance the security of agencies, which shall include—

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

(2) an evaluation of—

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

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

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede agency operations and mission delivery, threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

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

SEC. ____22. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

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

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

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

(1) collecting, organizing, and analyzing agency information system data in real time, including endpoint detection and response capabilities;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans, including alignment with existing shared services operations and policy.

(d) PILOT PROGRAM.—

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

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

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 270 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

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

(A) the agreement; and

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

SEC. ___23. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) EXEMPTION FROM FEDERAL REQUIREMENTS.—Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended—

(1) by redesignating paragraph (3) as paragraph (4); and

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

''(3) DURATION OF CERTIFICATION.—

''(A) IN GENERAL.—A certification and corresponding exemption of an agency under paragraph (2) shall expire on the date that is 4 years after the date on which the head of the agency submits the certification under paragraph (2)(A).

''(B) RENEWAL.—Upon the expiration of a certification of an agency under paragraph (2), the head of the agency may submit an additional certification in accordance with that paragraph.''.

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by section ___03(c) of this division, is 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 section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) that is effective on the date of submission of the report, the number of agency information systems that have received an exemption from those requirements.''.

(c) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date that is 1 year after the date of enactment of this Act.

SA 5816. Ms. MURKOWSKI (for herself and Mr. KING) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1077. ARCTIC SHIPPING FEDERAL ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Transportation shall establish the Arctic Shipping Federal Advisory Committee, as required in section 8426 of the Elijah E. Cummings Coast Guard Authorization Act of 2020 (division G of Public Law 116–283).

(b) FUNDING.—The Secretary of Transportation shall make available to the Arctic Shipping Advisory Committee, from amounts appropriated to the Office of the Secretary of Transportation, such funds as may be necessary for the operation and sustainment of the Committee.

SA 5817. Ms. MURKOWSKI (for herself and Mr. KING) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1077. AMENDMENTS TO THE ARCTIC RESEARCH AND POLICY ACT OF 1984.

(a) FINDINGS AND PURPOSES.—Section 102(a) of the Arctic Research and Policy Act of 1984 (15 U.S.C. 4101(a)) is amended—

(1) in paragraph (2), by inserting ''and homeland'' after ''national'';

(2) by redesignating paragraphs (5) through (17) as paragraphs (6) through (18), respectively;

(3) by striking paragraph (4) and inserting the following:

''(4) Changing Arctic conditions directly affect global weather and climate patterns and must be better understood—

''(A) to promote better agricultural management throughout the United States; and

''(B) to address the myriad of impacts, challenges, and opportunities brought about by such change.

''(5) Since a rapidly changing climate will reshape the economic, social, cultural, political, environmental, and security landscape of the Arctic region, sustained, robust, coordinated, reliable, appropriately funded, and dependable Arctic research is required to inform and influence sound domestic and international Arctic policy.''; and

(4) in paragraph (6), as redesignated, by inserting ''and climate'' after ''weather''.

(b) ARCTIC RESEARCH COMMISSION.—Section 103 of the Arctic Research and Policy Act of 1984 (15 U.S.C. 4102) is amended—

(1) in subsection (b)—

(A) in paragraph (1)(B)—

(i) by striking ''who are'' and inserting ''who is a''; and

(ii) by striking ''who live in areas'' and inserting ''who live in an area'';

(B) in paragraph (2), by striking ''chairperson'' and inserting ''Chair''; and

(2) in subsection (d)—

(A) in paragraph (1)—

(i) by inserting ''or her'' after ''his''; and

(ii) by inserting '', or in the case of the Chair, not to exceed 120 days of service each year'' after ''year''; and

(B) in paragraph (2), by striking ''Chairman'' and inserting ''Chair''.

(c) ADMINISTRATION OF THE COMMISSION.—Section 106(4) of the Arctic Research and Policy Act of 1984 (15 U.S.C. 4105(4)) is amended—

(1) by inserting '', and other Federal Government entities, as appropriate,'' after ''with the General Services Administration''; and

(2) by inserting '', or the heads of other Federal Government entities, as appropriate,'' before the semicolon.

(d) INTERAGENCY ARCTIC RESEARCH POLICY COMMITTEE.—Section 107(b)(2) of the Arctic Research and Policy Act of 1984 (15 U.S.C. 4106(b)(2)) is amended—

(1) by redesignating subparagraph (L) as subparagraph (O); and

(2) in subparagraph (K), by striking ''and'' at the end; and

(3) by inserting after subparagraph (K) the following:

''(L) the Department of Agriculture;

''(M) the Marine Mammal Commission;

''(N) the Denali Commission; and''.

(e) 5-YEAR ARCTIC RESEARCH PLAN.—Section 109(a) of the Arctic Research and Policy Act of 1984 (15 U.S.C. 4108(a)) is amended by striking ''The Plan'' and inserting ''Notwithstanding section 3003 of the Federal Reports Elimination and Sunset Act of 1995 (Public Law 104–66), the Plan''.

SA 5818. Ms. MURKOWSKI (for herself and Mr. KING) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle F of title X, add the following:

SEC. 1064. REPORT ON ESTABLISHING PRESENCE OF NAVY OR COAST GUARD IN THE UNITED STATES ARCTIC.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Commandant of the Coast Guard and the Chief of Naval Operations shall jointly submit a report to the appropriate committees of Congress that—

(1) describes the requirements necessary to establish, and the feasibility of establishing, a year-round presence of the Navy and the Coast Guard in the Arctic region at—

(A) the Port of Nome;

(B) the natural deepwater port of Unalaska;

(C) the former Coast Guard Station at Port Clarence;

(D) Point Spencer (as defined in section 532 of the Pribilof Island Transition Completion Act of 2015 (subtitle B of title V of Public Law 114–120));

(E) the port on Saint George Island in the Bering Sea;

(F) the Port of Adak;

(G) Cape Blossom;

(H) Southeast Alaska;

(I) ports in the Northeastern United States including Eastport, Searsport, and Portland; and

(J) any other deepwater port that the Commandant determines would facilitate such a presence in the places described in subparagraphs (A) through (I); and

(2) provides an estimate of the costs of implementing the requirements described in paragraph (1), after taking into account the costs of constructing the onshore infrastructure that will be required to support year-